1003650 • 06804360

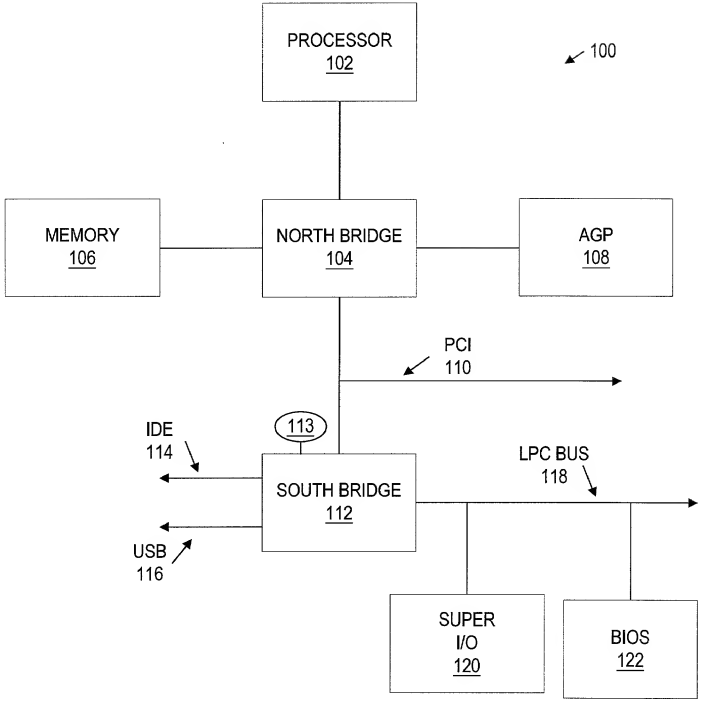


Fig. 1A
(Prior Art)

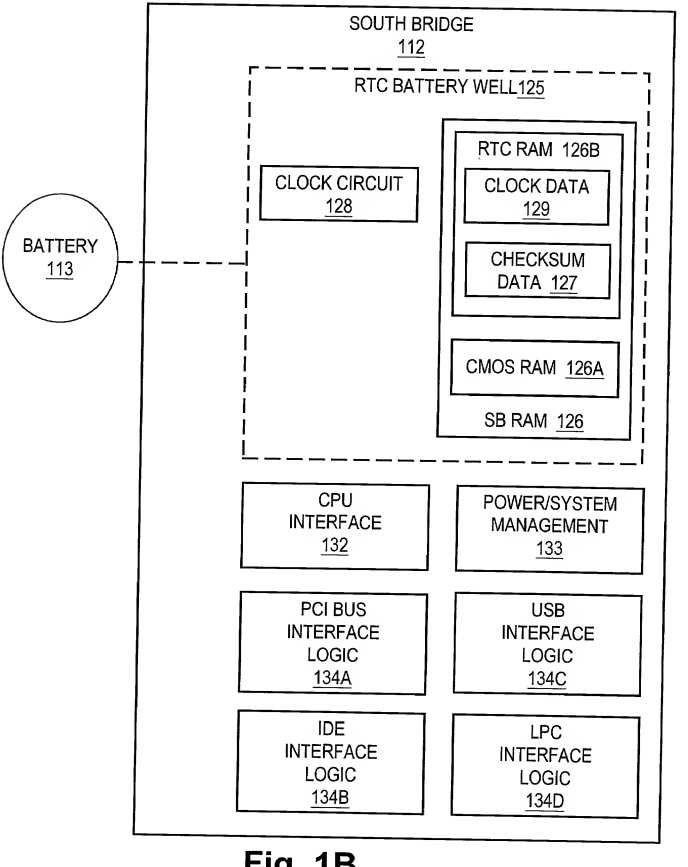
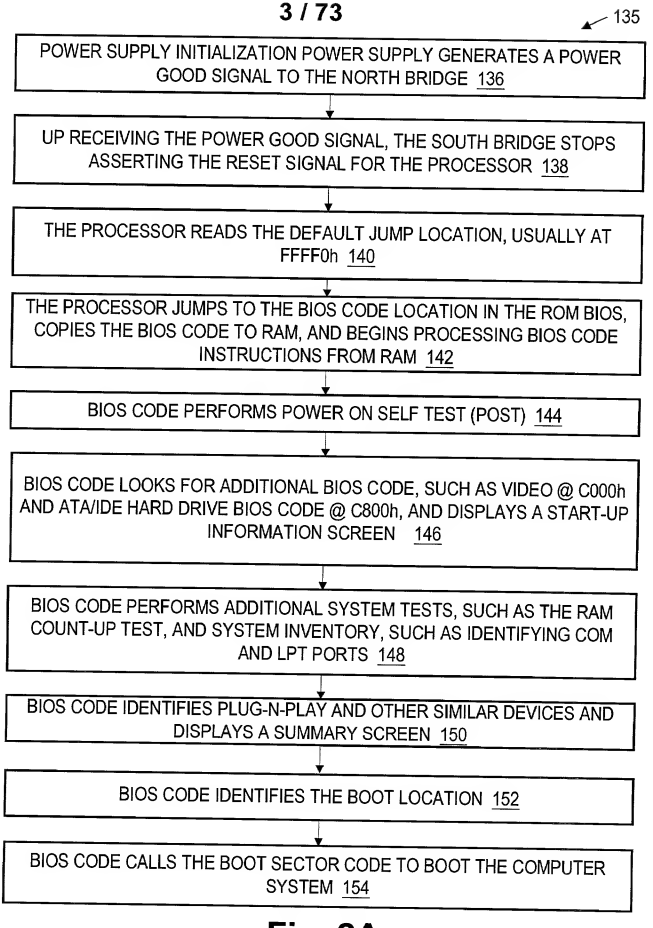


Fig. 1B
(Prior Art)

TT0550 • 0680/7860



0980.0550.0068.0980

Fig. 2A
(Prior Art)

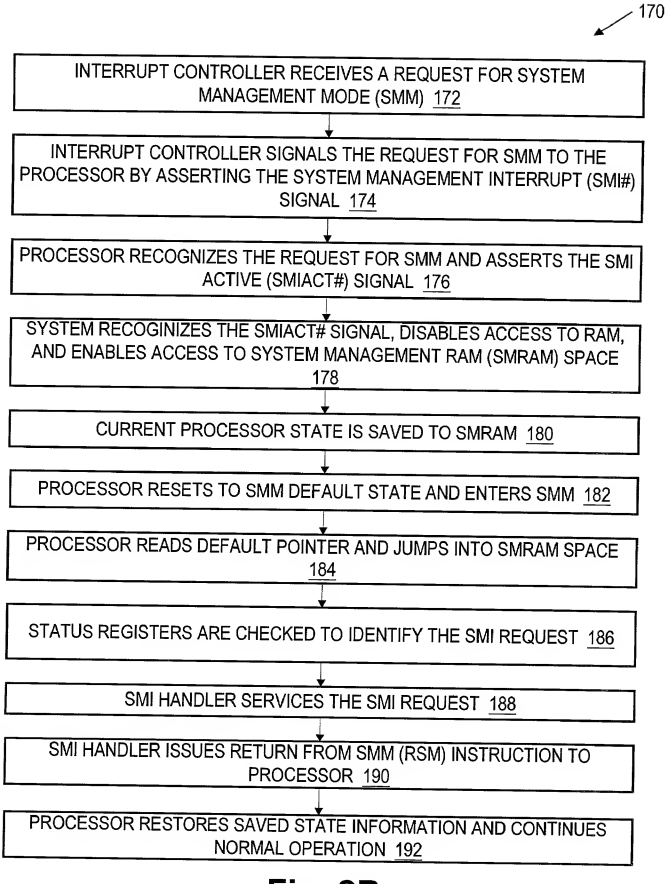


Fig. 2B
(Prior Art)

TT04S0"06807860

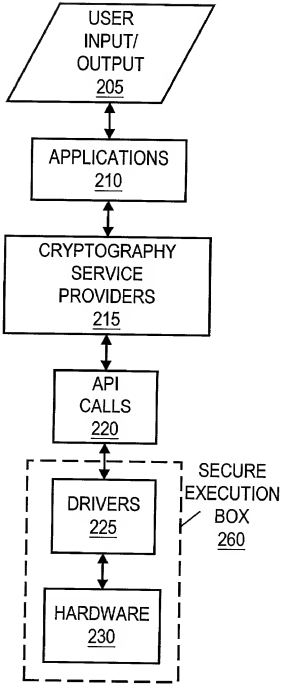


Fig. 3

T0050"06807860

0998708 * 05300 1

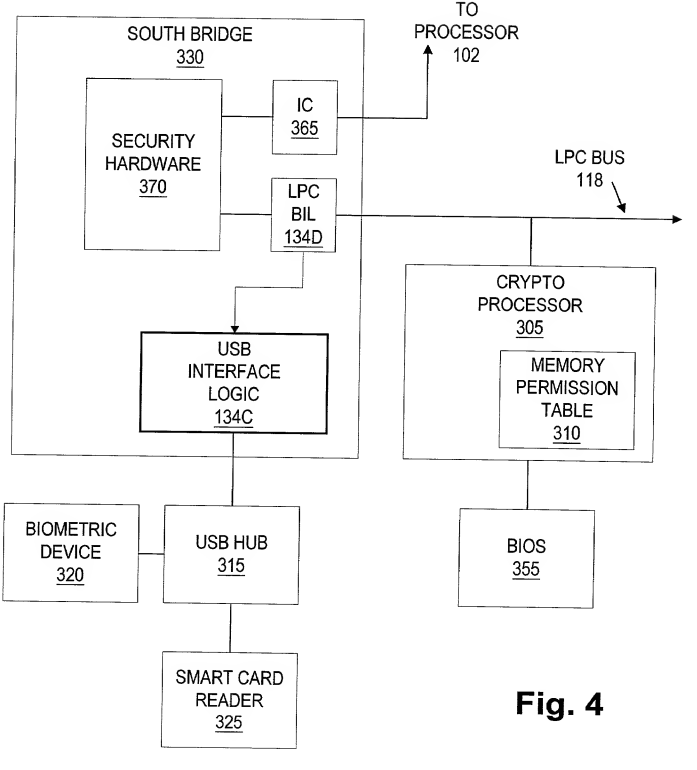


Fig. 4

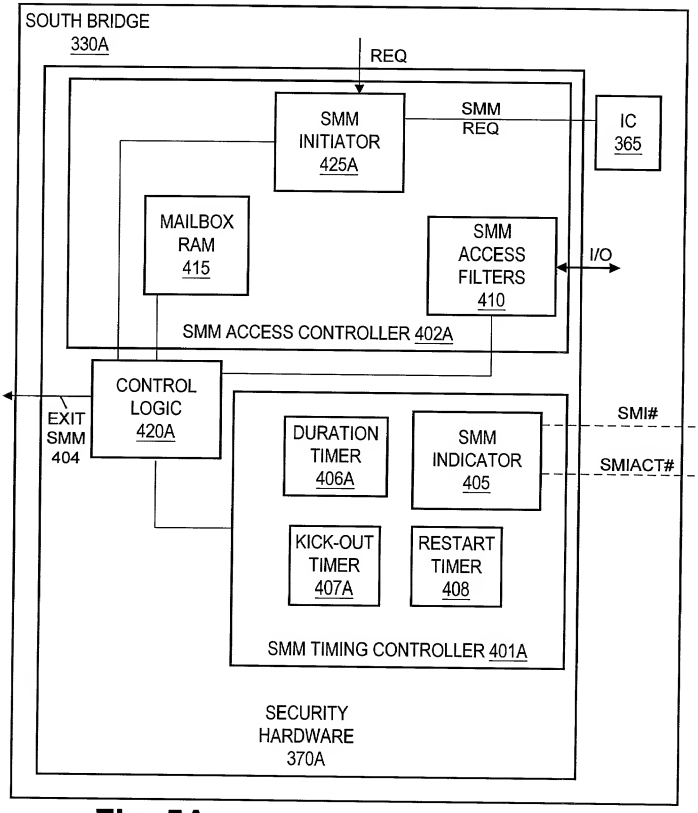


Fig. 5A

0980708860 "05001

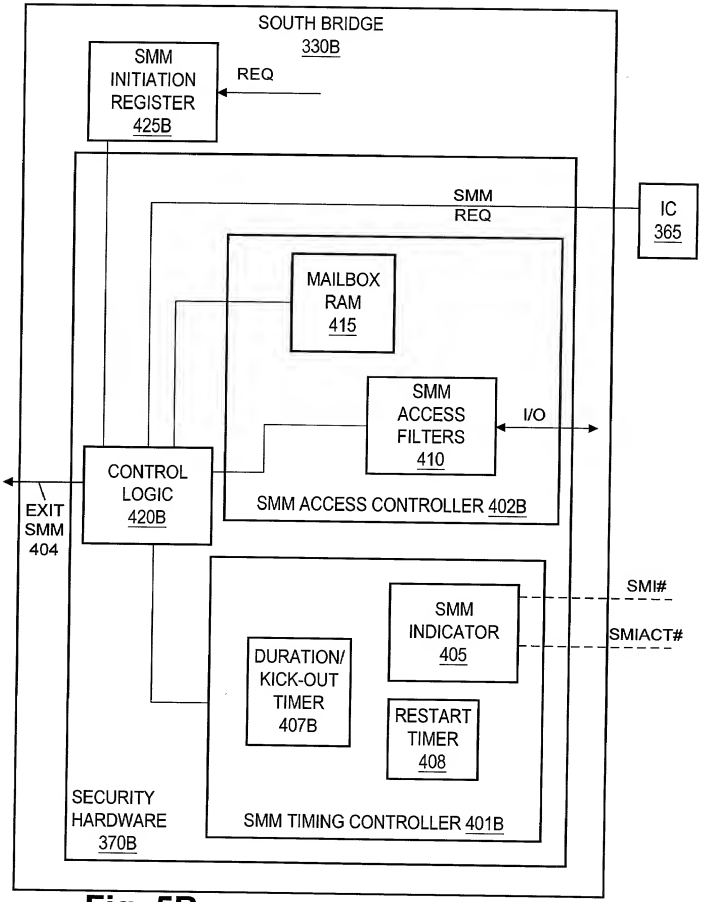


Fig. 5B

TT0850*06807860

TOOES0 '0680780

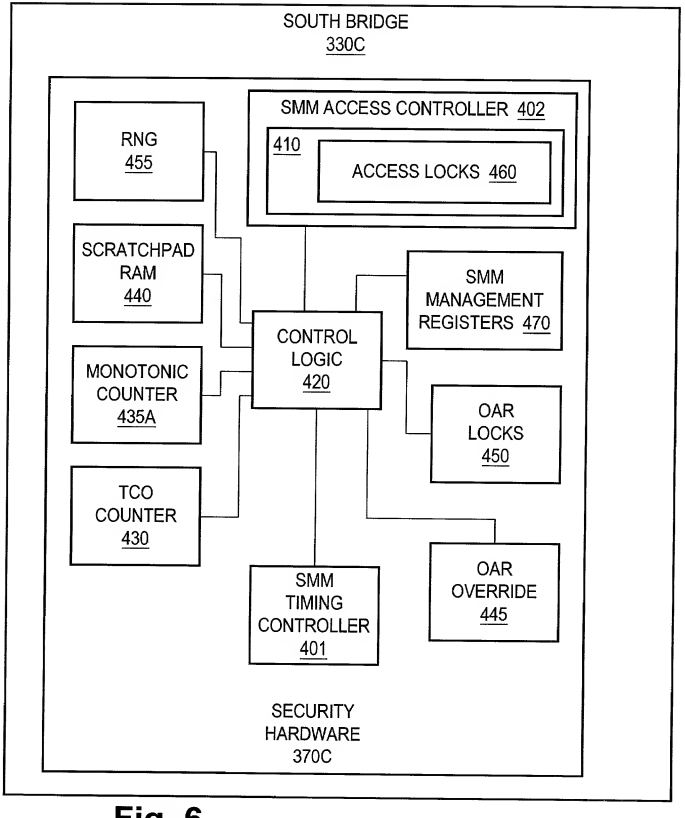


Fig. 6

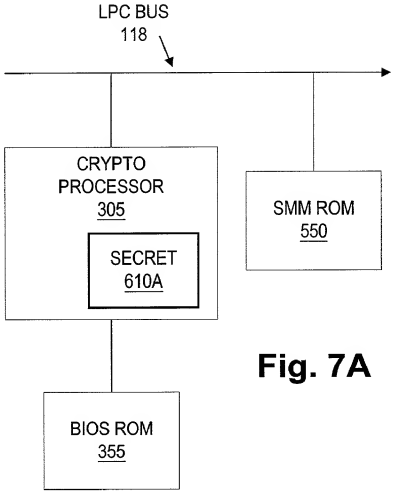


Fig. 7A

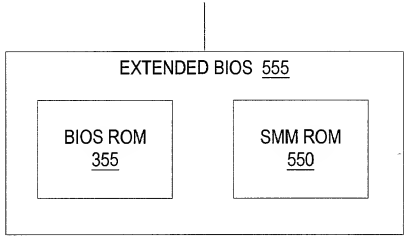


Fig. 7B

0987089D.050301

1005.0 * 06807860

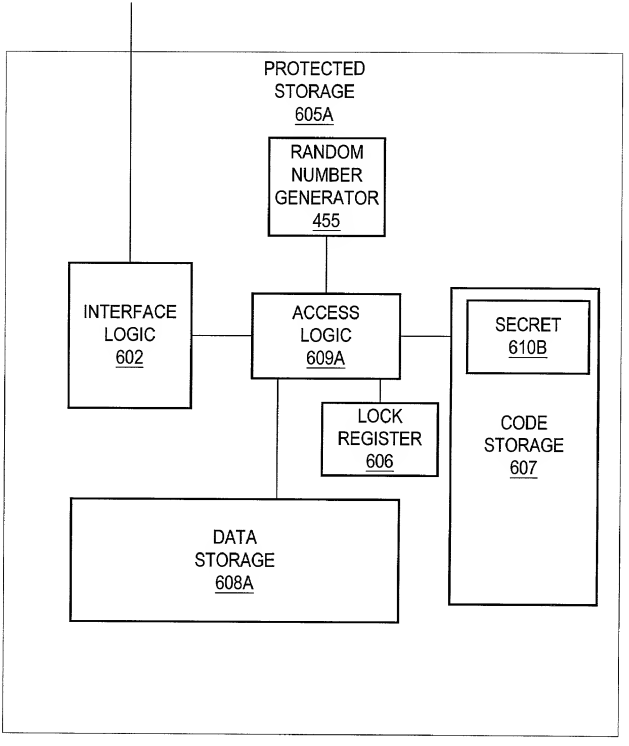
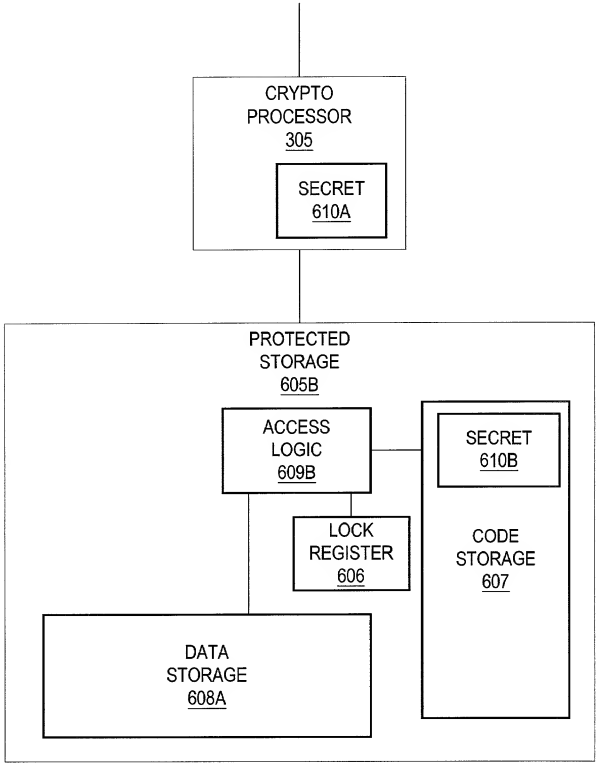


Fig. 7C



0980808.05300L

Fig. 7D

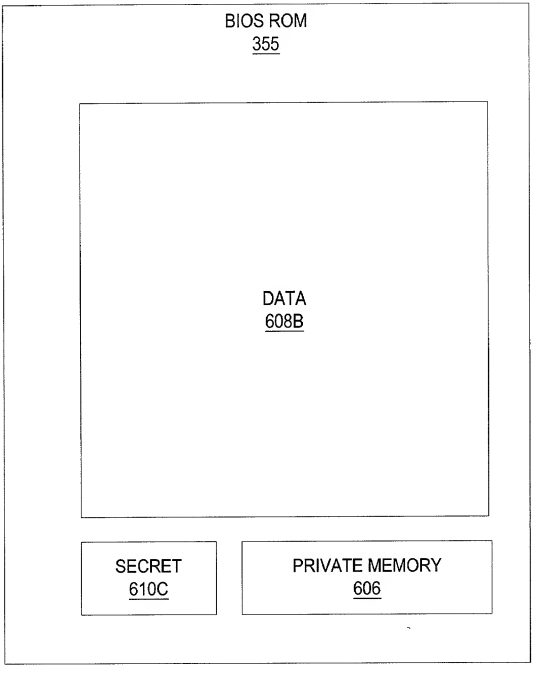


Fig. 8A

0980708901 · 05500101

0980890.05300.1

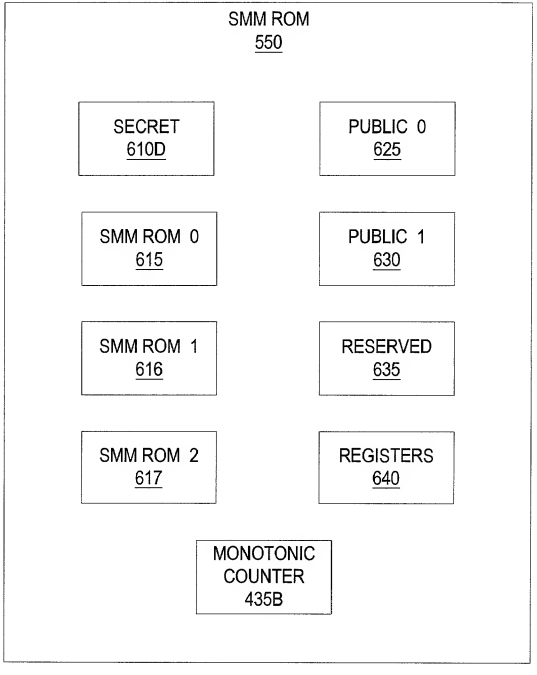
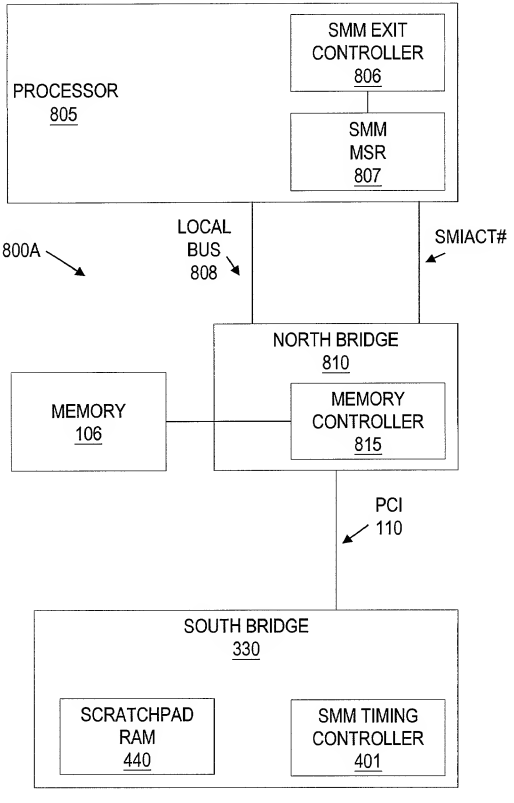


Fig. 8B



0983708890.053001

Fig. 9A

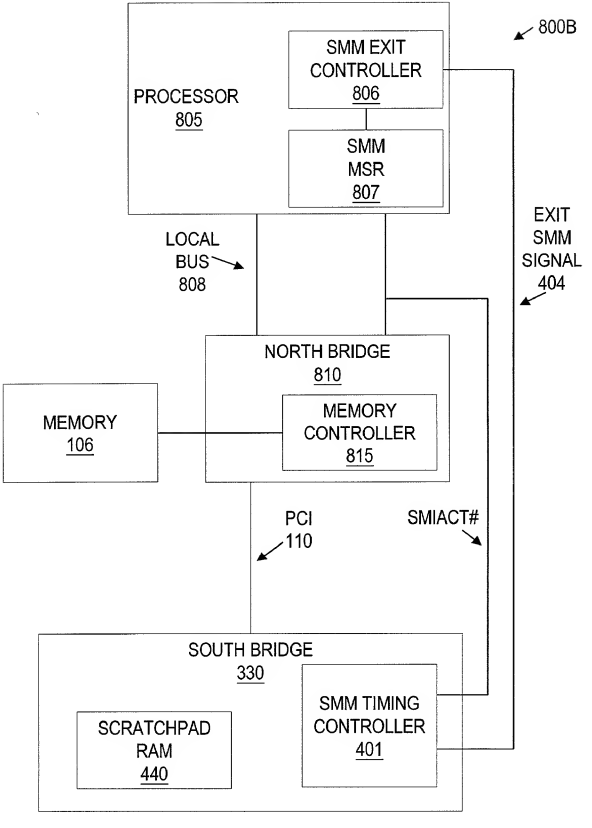


Fig. 9B

10030501.080700

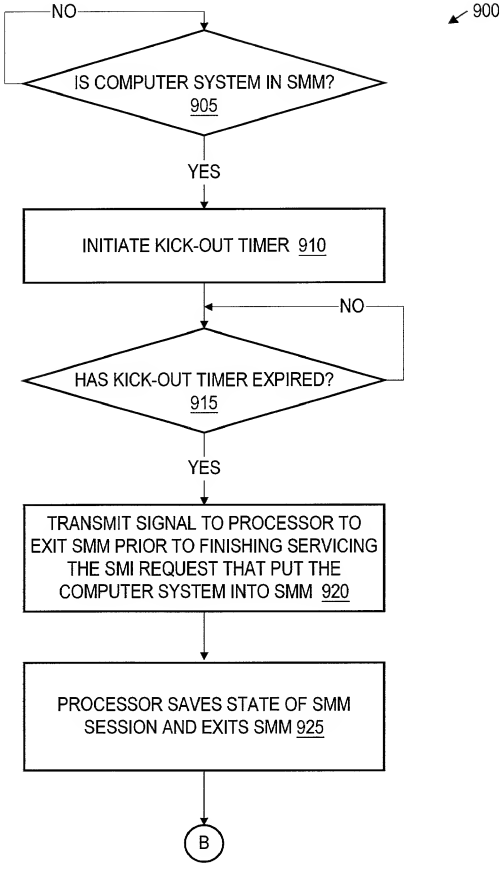


Fig. 10A

TT0350 * 06802860

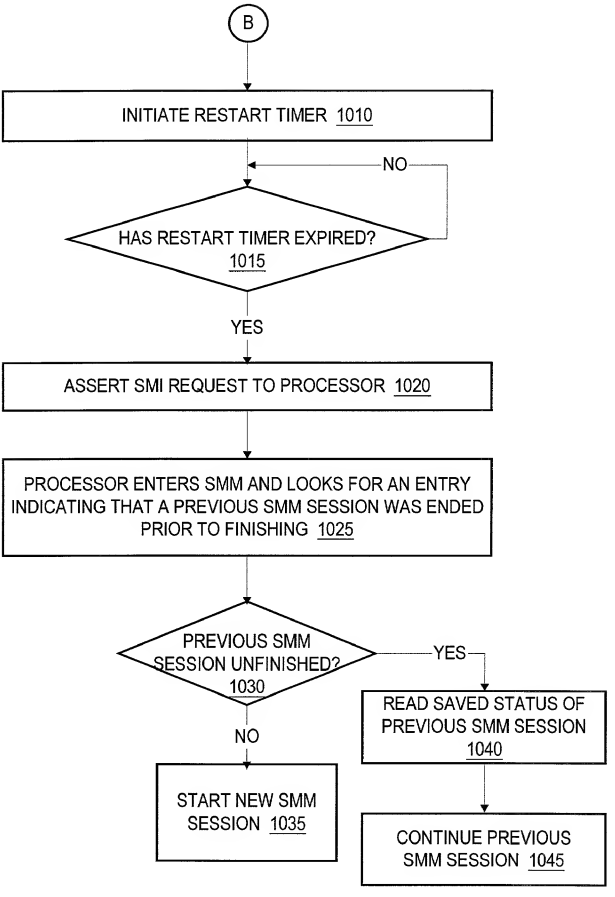


Fig. 10B

"0080708990"

0987.0890.053001

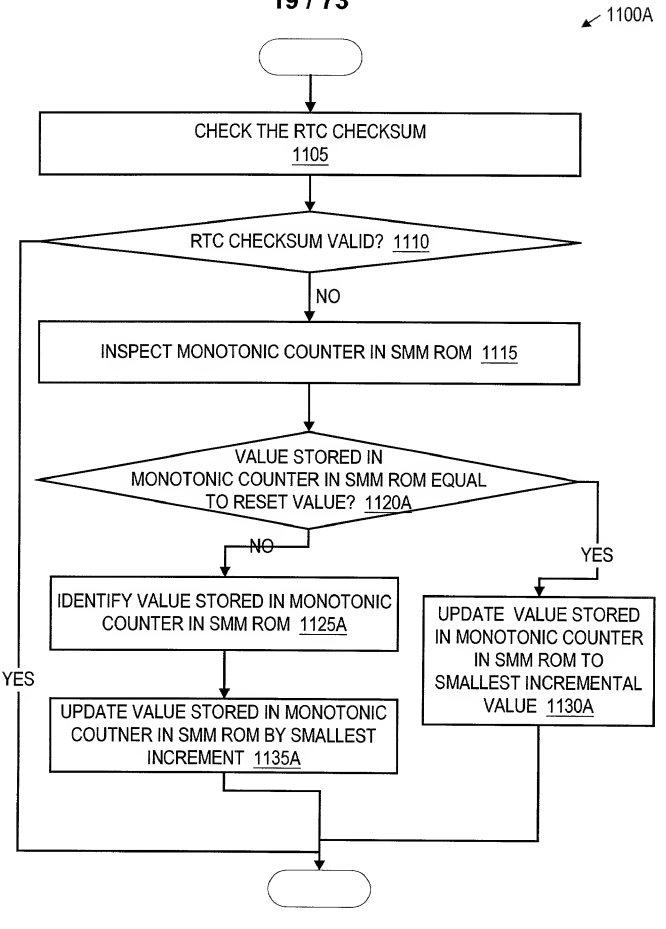


Fig. 11A

09870890 - 053001

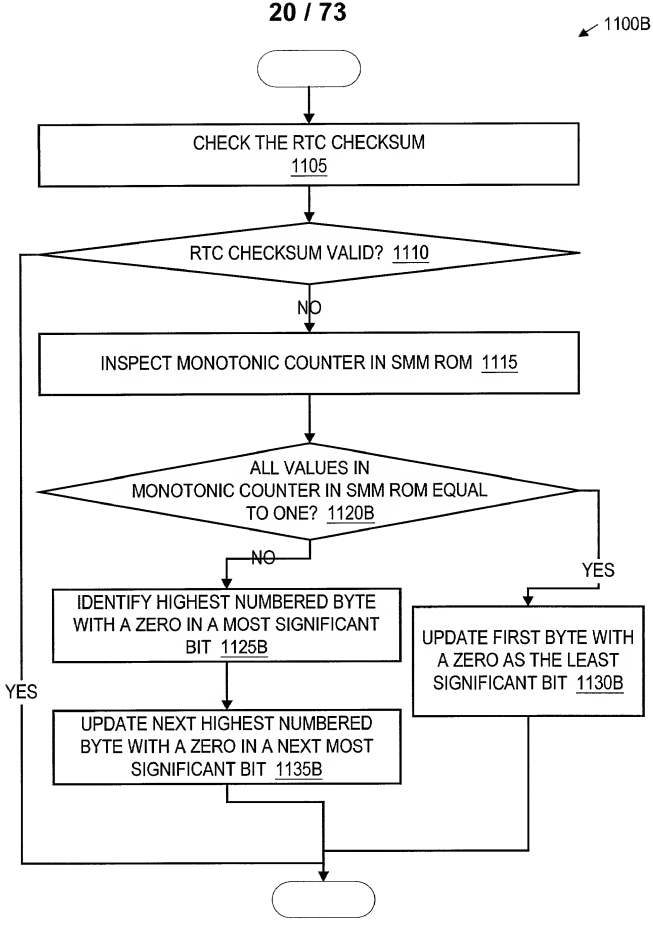


Fig. 11B

TT0850*06807A360

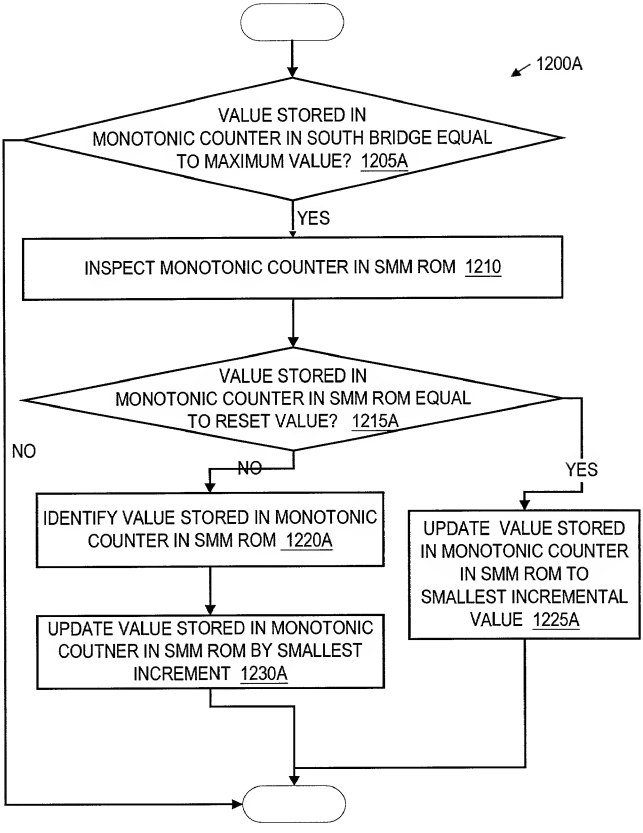


Fig. 12A

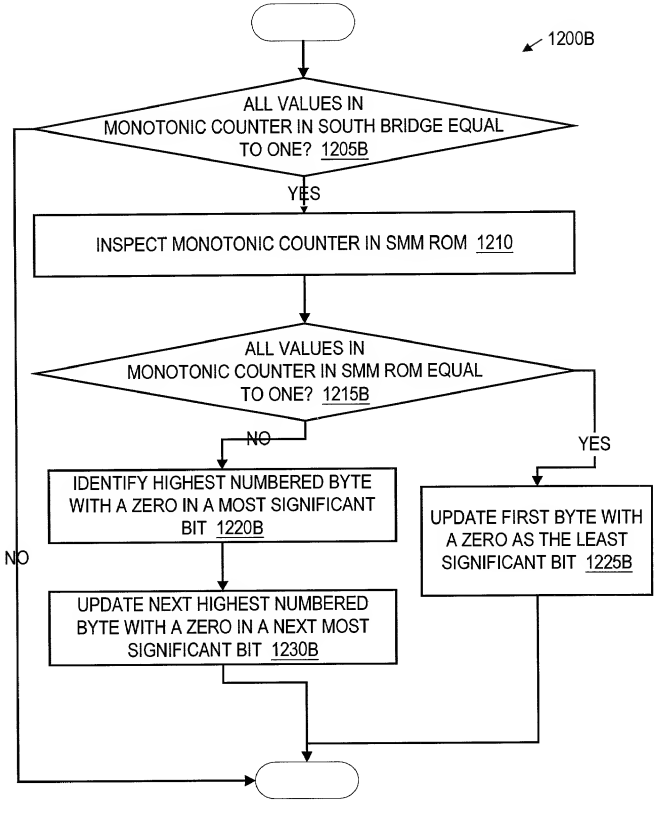

1200B
ALL VALUES IN MONOTONIC COUNTER IN SOUTH BRIDGE EQUAL TO ONE? 1205B
YES
INSPECT MONOTONIC COUNTER IN SMM ROM 1210
ALL VALUES IN MONOTONIC COUNTER IN SMM ROM EQUAL TO ONE? 1215B
NO
YES
IDENTIFY HIGHEST NUMBERED BYTE WITH A ZERO IN A MOST SIGNIFICANT BIT 1220B
UPDATE FIRST BYTE WITH A ZERO AS THE LEAST SIGNIFICANT BIT 1225B
NO
UPDATE NEXT HIGHEST NUMBERED BYTE WITH A ZERO IN A NEXT MOST SIGNIFICANT BIT 1230B

Fig. 12B

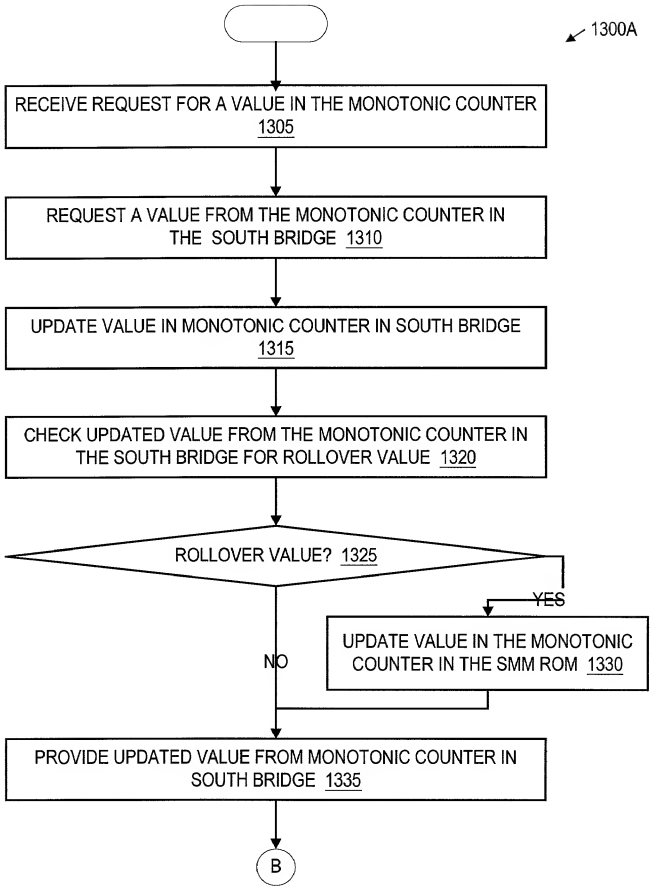
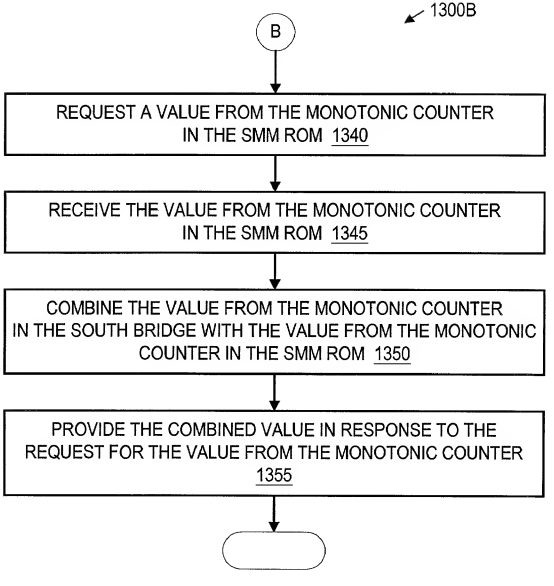


Fig. 13A

TT0829.0550.0990708.01



1000550 * 06307860

Fig. 13B

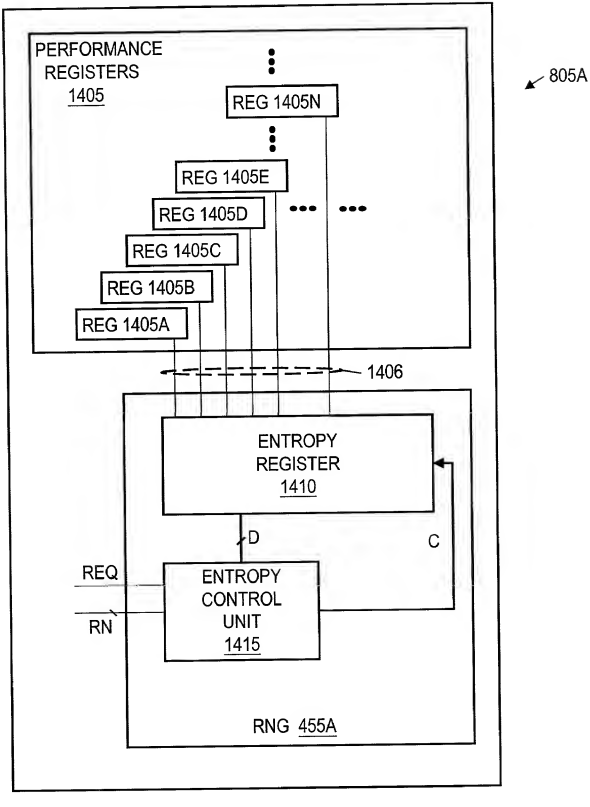


Fig. 14A

0988708900.055301

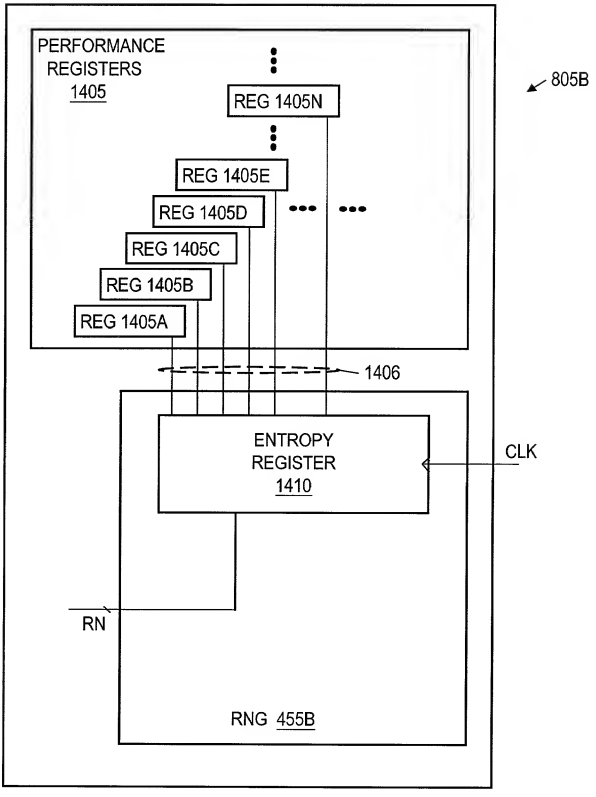


Fig. 14B

0980/0890.05300.1

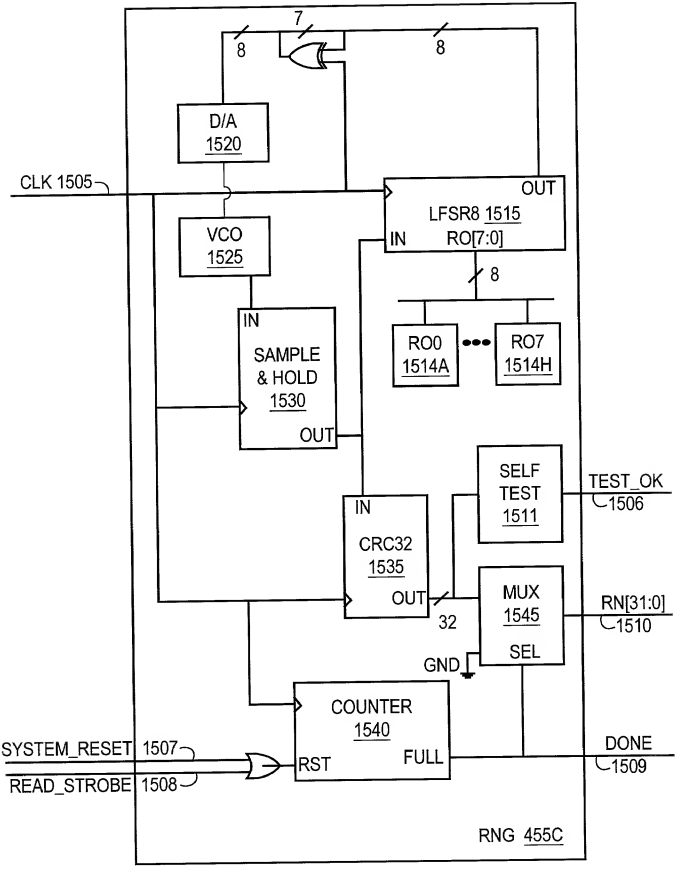

7
8
8
D/A
1520
CLK 1505
OUT
LFSR8 1515
IN
RO[7:0]
VCO
1525
8
IN
SAMPLE
& HOLD
1530
OUT
RO0
1514A
RO7
1514H
SELF
TEST
1511
TEST_OK
1506
IN
CRC32
1535
OUT
32
MUX
1545
SEL
RN[31:0]
1510
GND
COUNTER
1540
SYSTEM_RESET 1507
READ_STROBE 1508
RST
FULL
DONE
1509
RNG 455C

Fig. 15

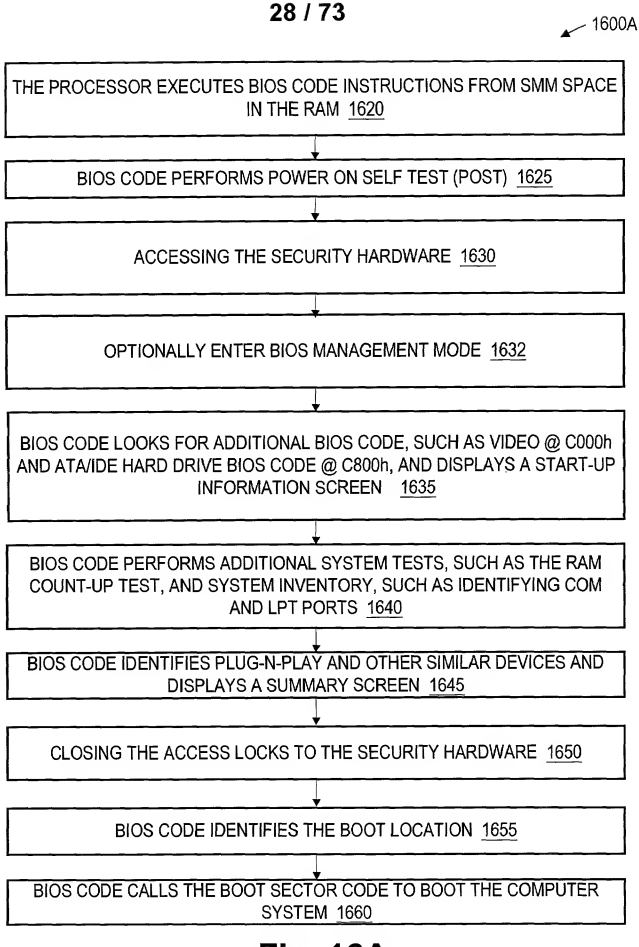
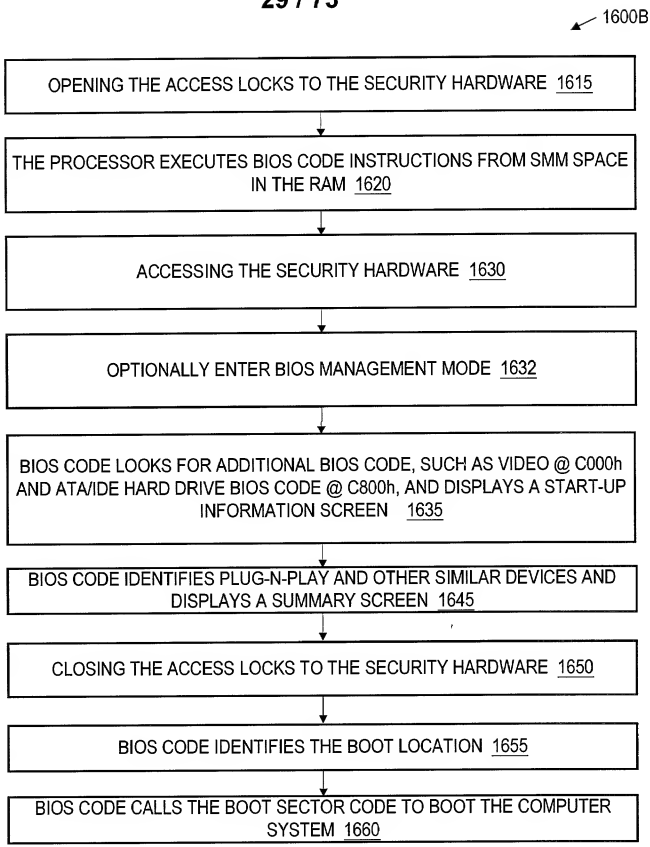


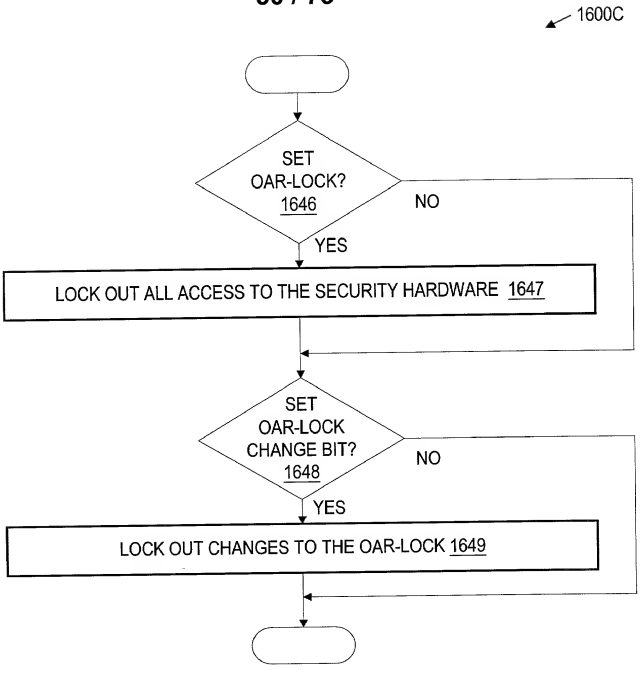
Fig. 16A

"0850.0880/860



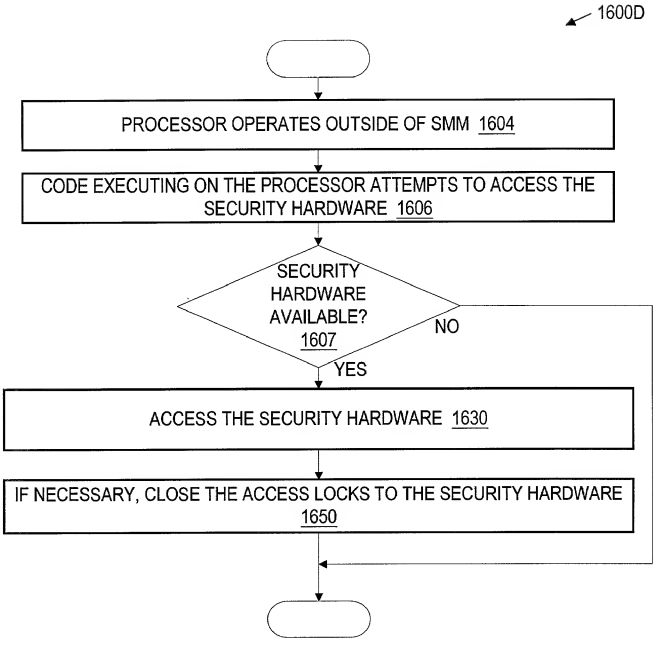
0938708690.053001

Fig. 16B



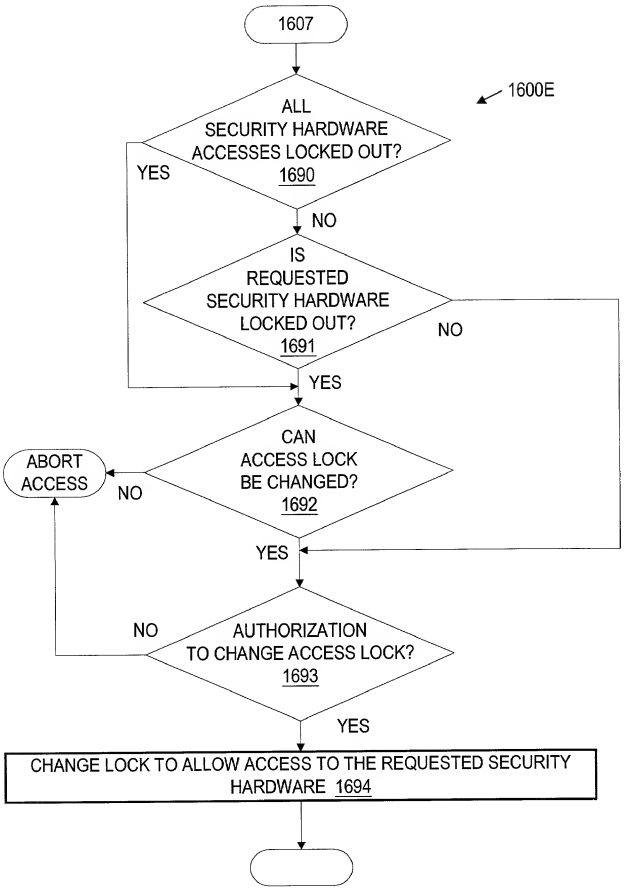
TT0E50"06807860

Fig. 16C



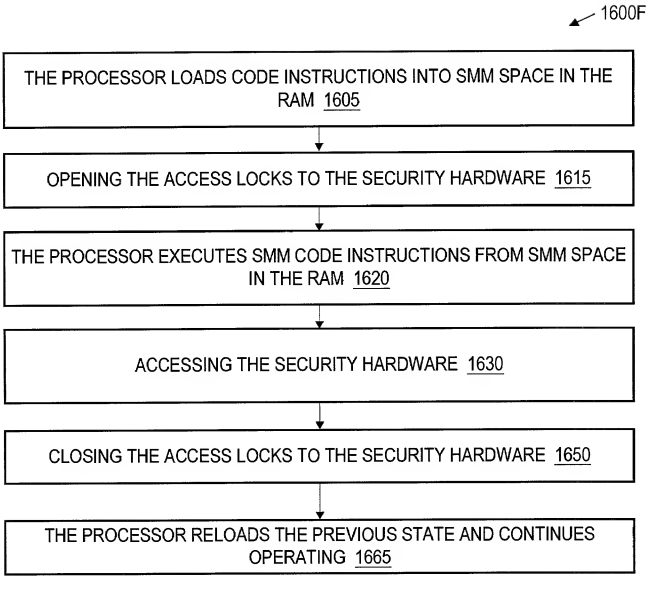
TT0850 * 06807860

Fig. 16D



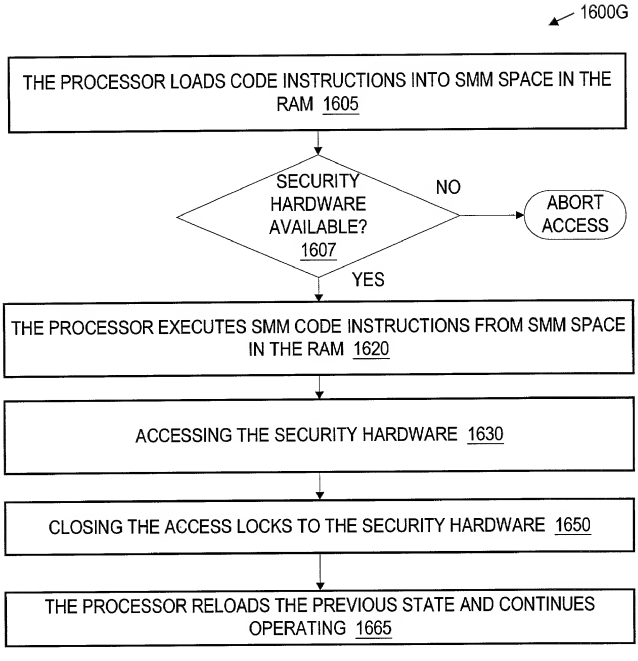
0918708910 * 053001

Fig. 16E



1000050*0680780

Fig. 16F



10003.0508/2860

Fig. 16G

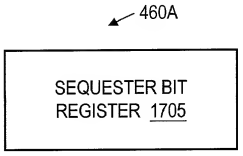


Fig. 17A

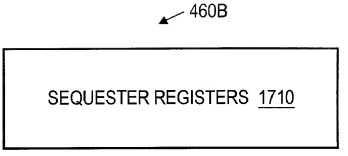


Fig. 17B

05300101 • 0538708

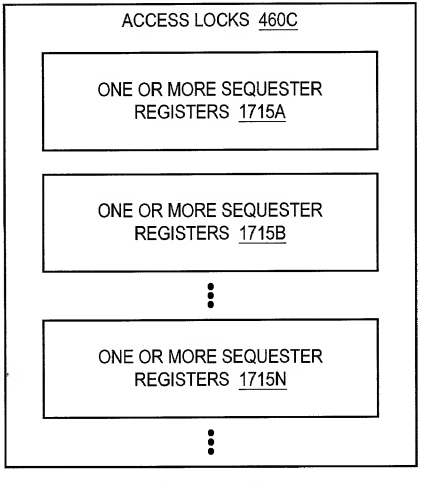


Fig. 17C

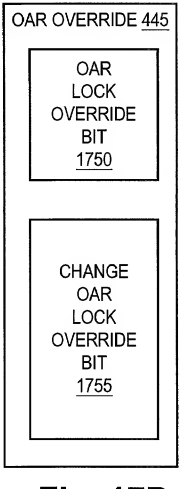


Fig. 17D

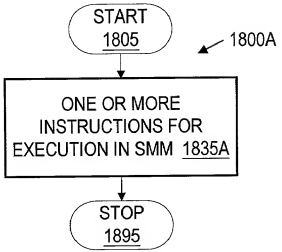


Fig. 18A
PRIOR ART

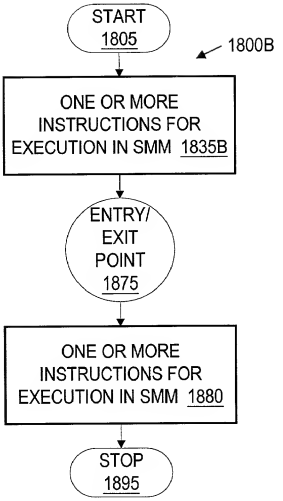


Fig. 18B

1006250 "06807860

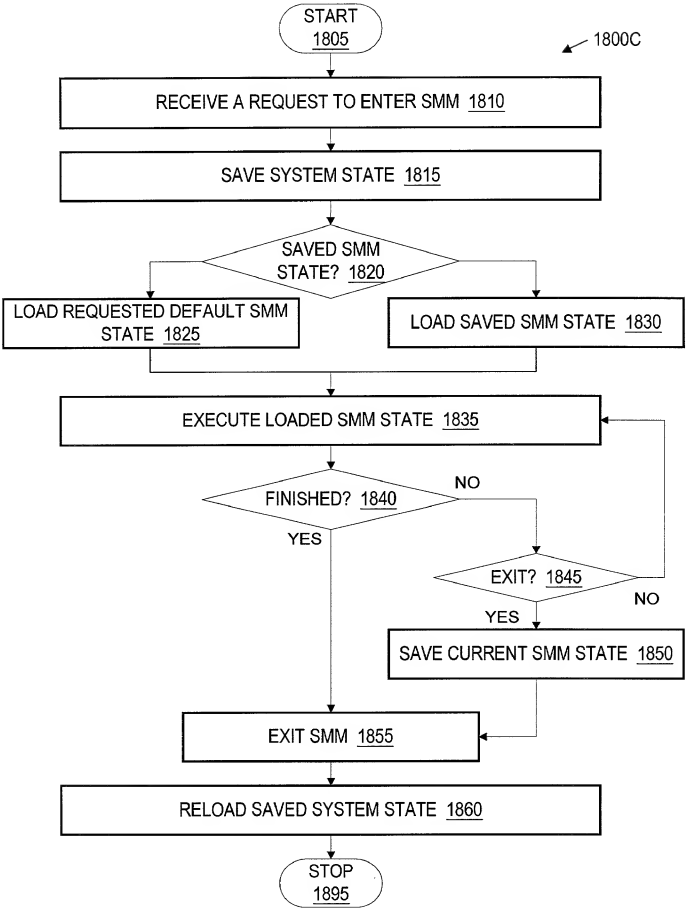
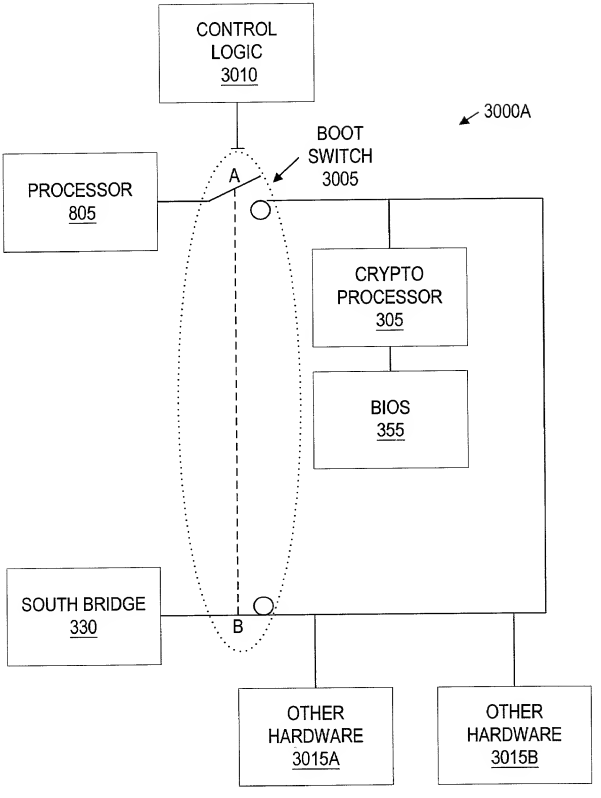


Fig. 18C

0980703-0553001



0053001 · 0680/7890

Fig. 19A

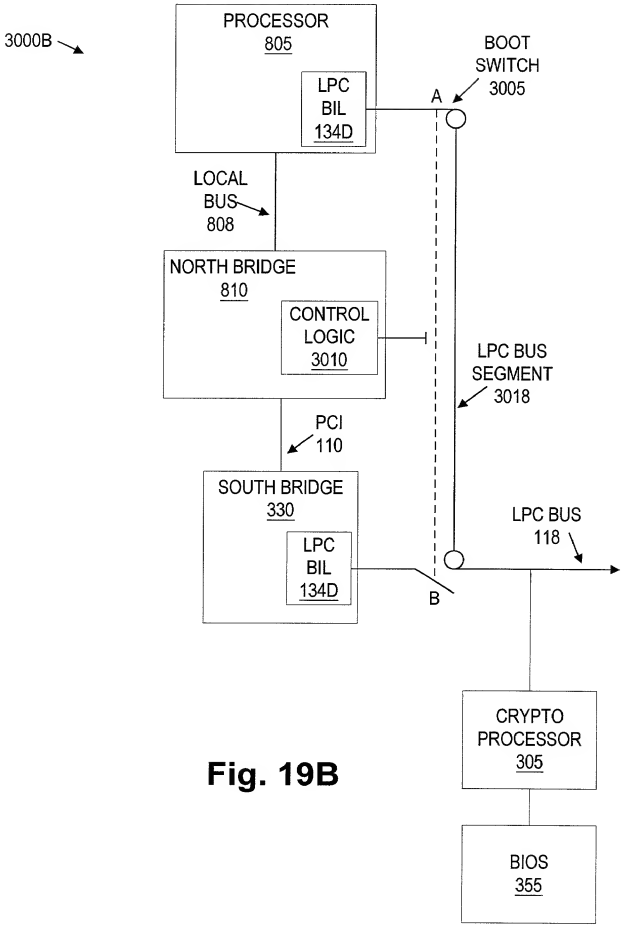
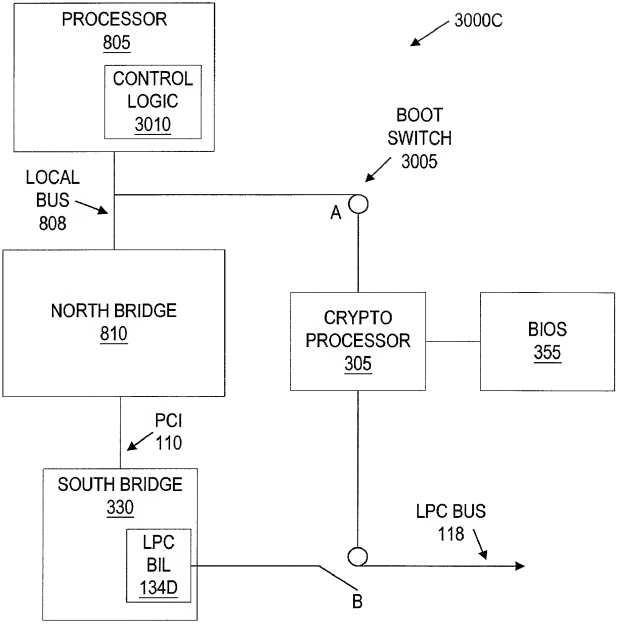


Fig. 19B

100E50 - 0680/860



10003.50.06807860

Fig. 19C

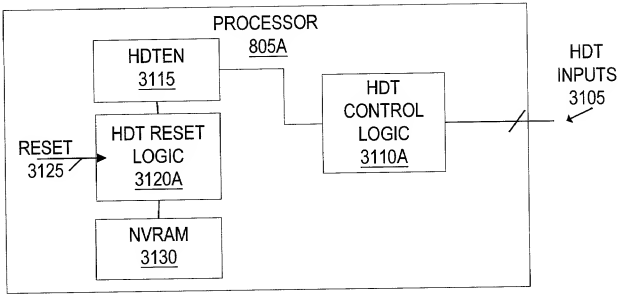


Fig. 20A

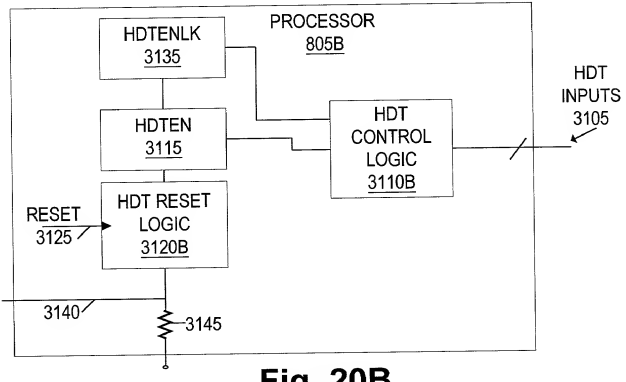


Fig. 20B

0987089D.053001

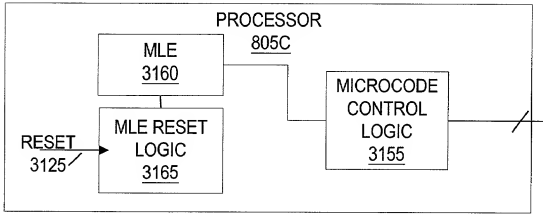


Fig. 20C

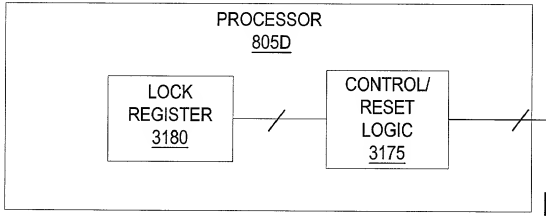


Fig. 20D

TOOES0"0680/860

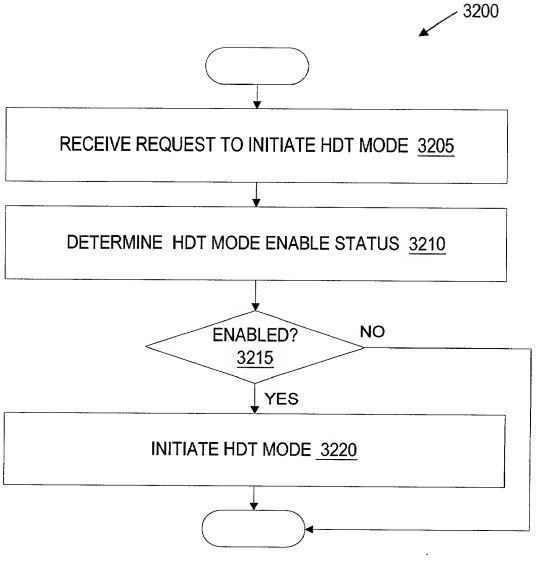
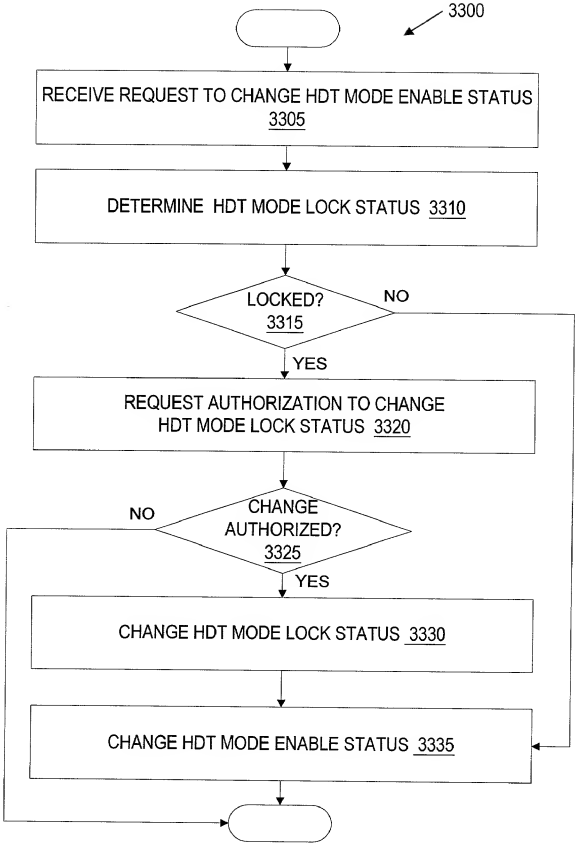


Fig. 21

0928/0890.05300.1



T0050*0680/860

Fig. 22

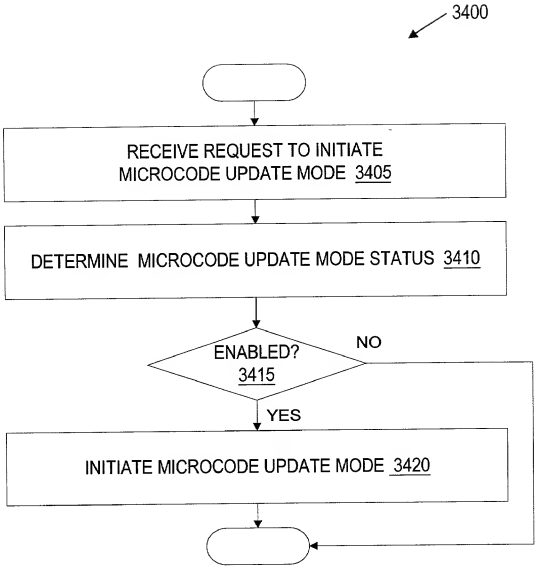
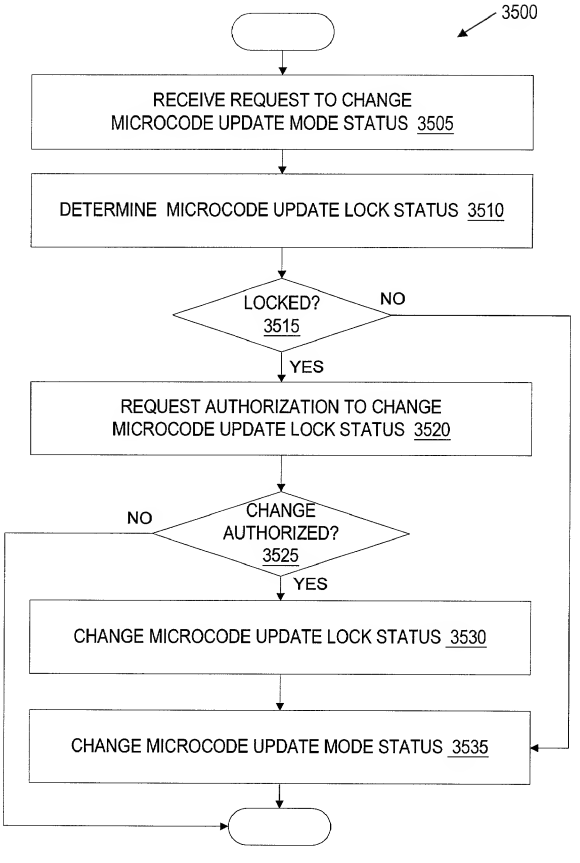


Fig. 23

0987089D.053001



0080780.05301

Fig. 24

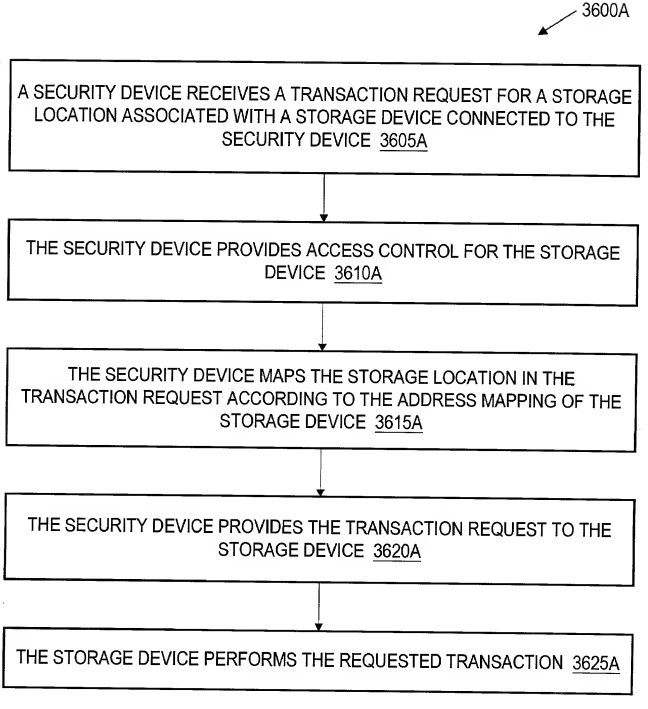


Fig. 25A

05300108907890

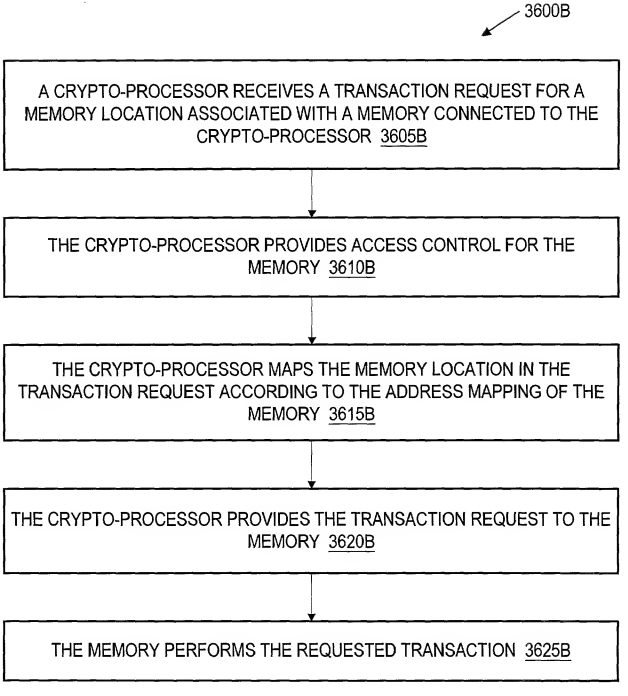
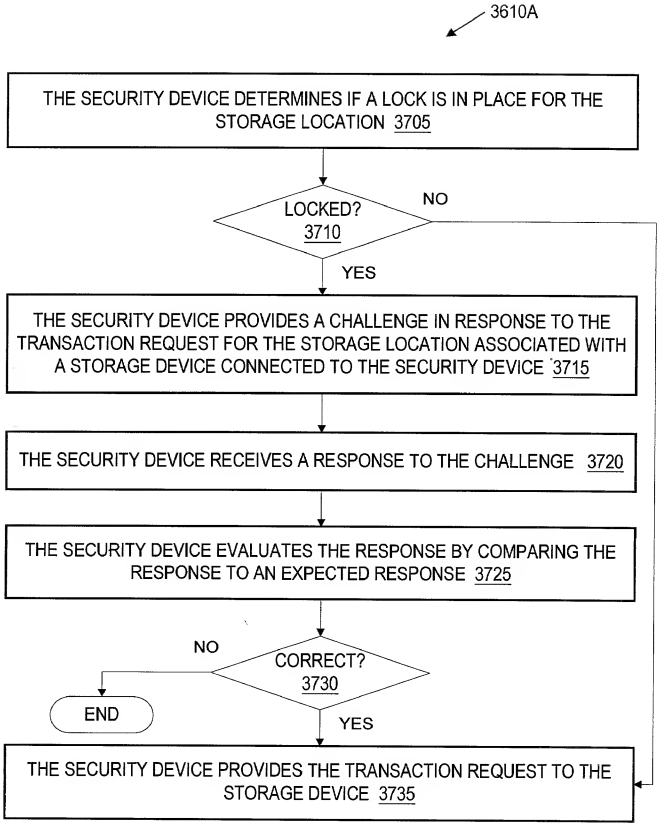


Fig. 25B

T0050*06802860



T0050*06807860

Fig. 26

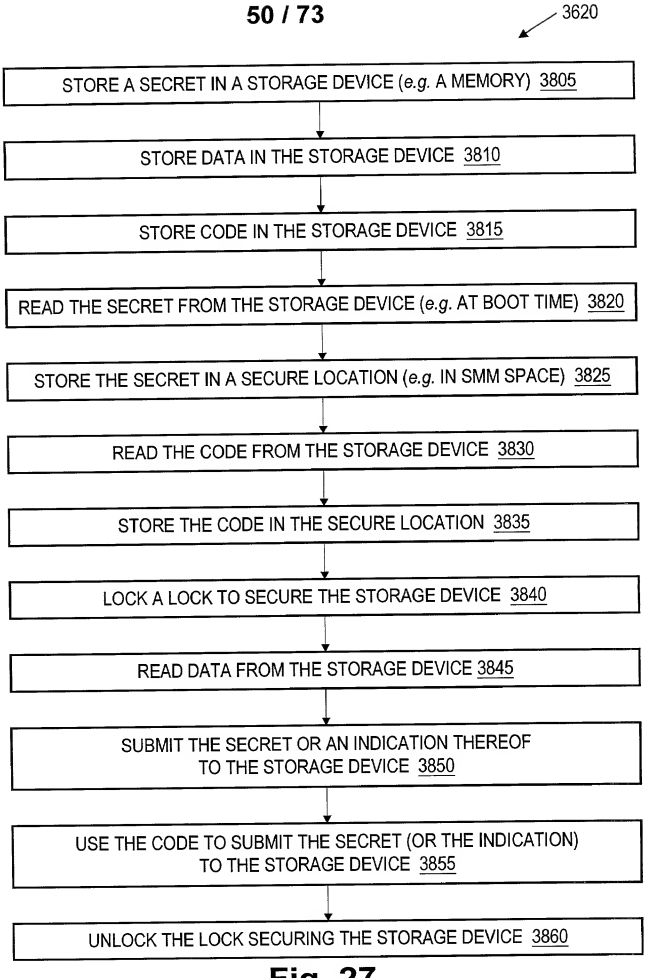
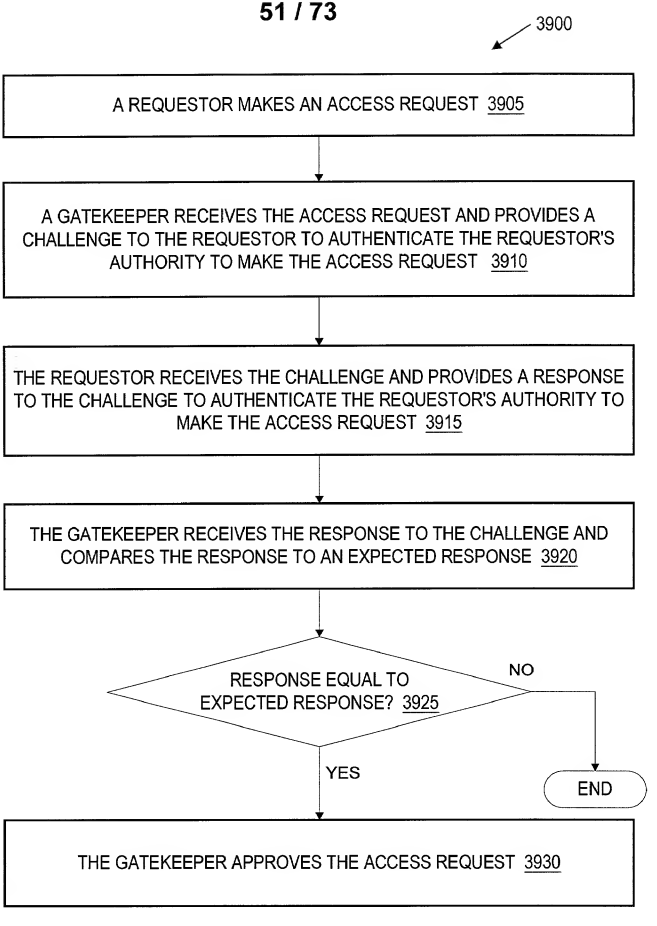


Fig. 27

0980780.05301



TOOES0"06807860

Fig. 28
(Prior Art)

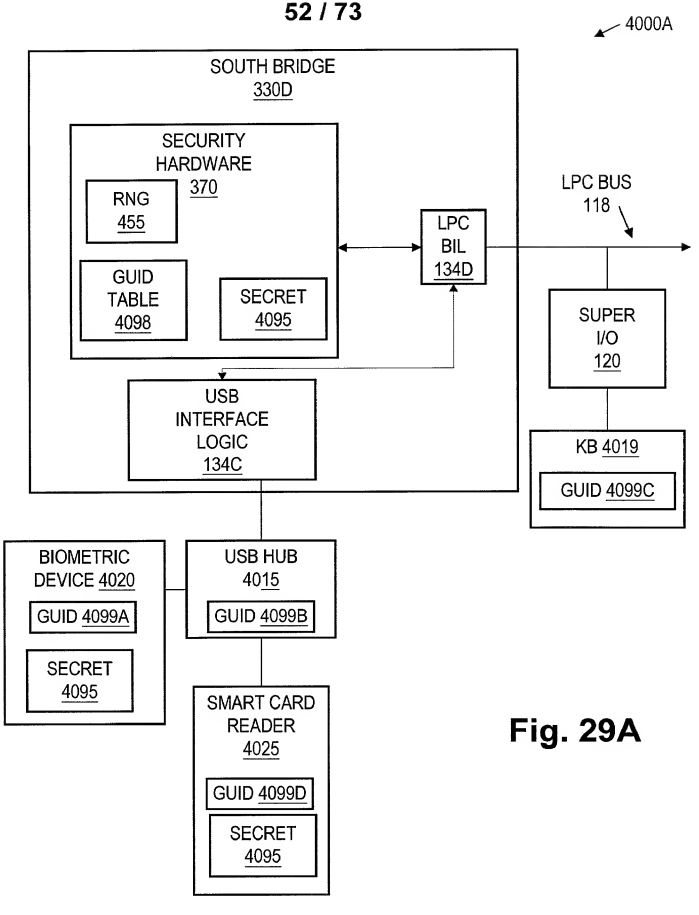


Fig. 29A

0987080910.050301

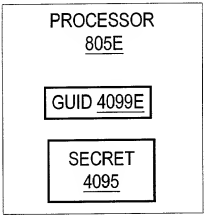


Fig. 29B

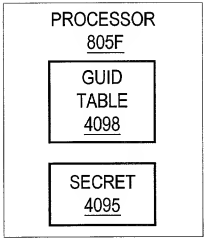


Fig. 29C

0987088990 - 053001

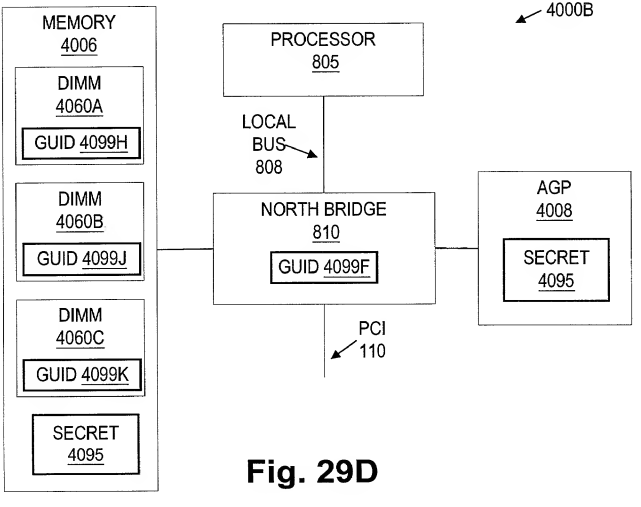


Fig. 29D

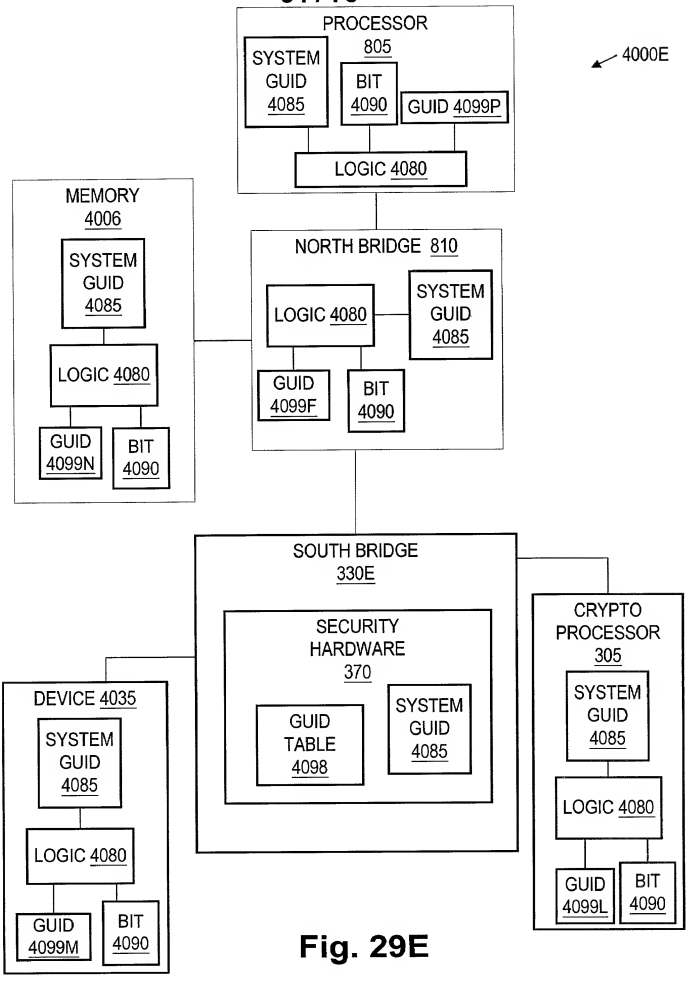


Fig. 29E

TT0E50*05804860

09870890.052001

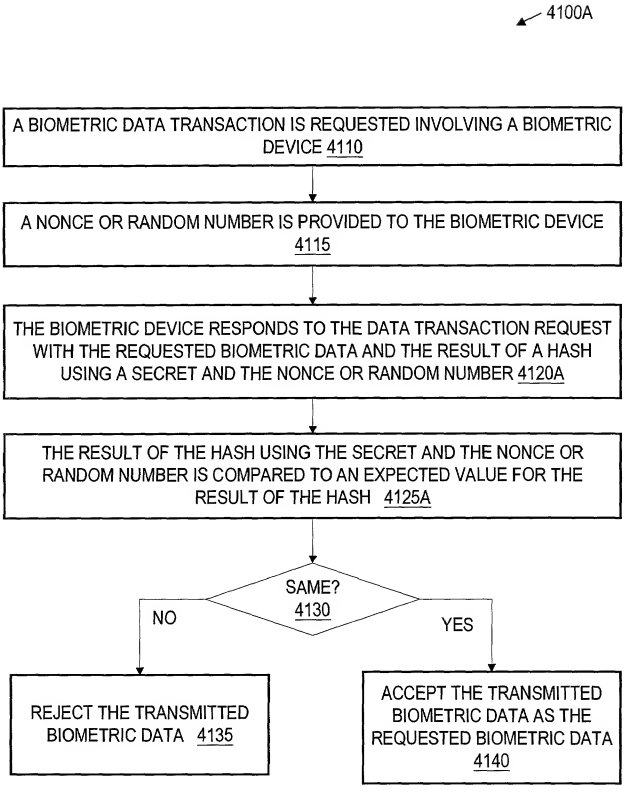
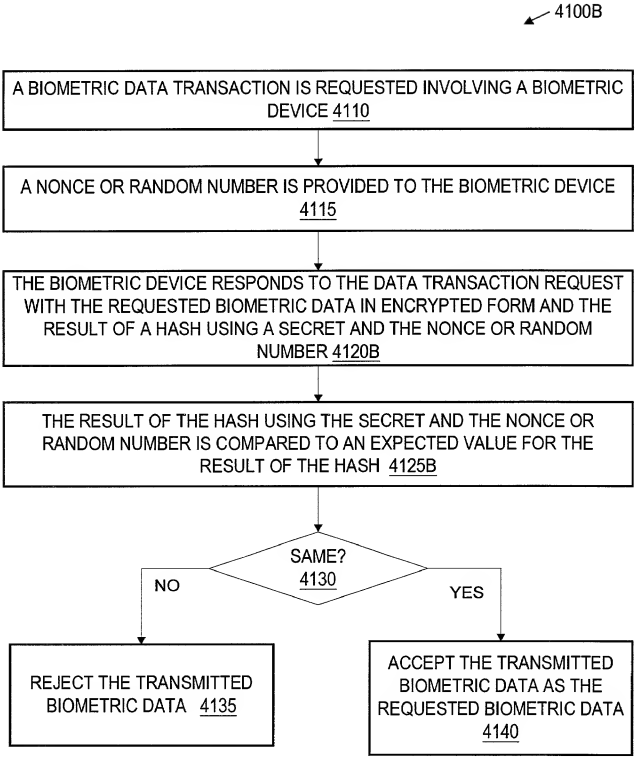
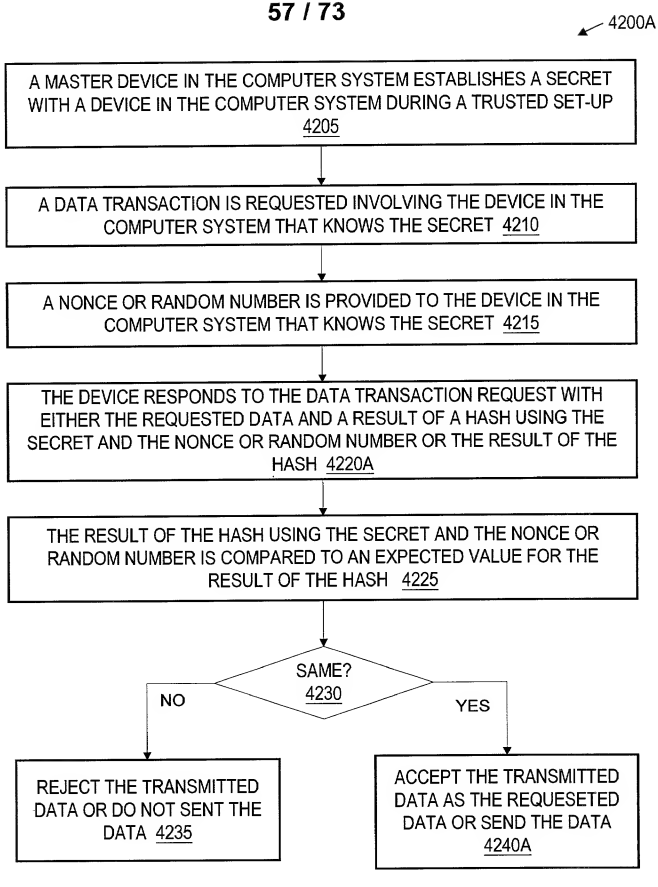


Fig. 30A



09870890 "05300"

Fig. 30B



"0080709.0530.01"

Fig. 31A

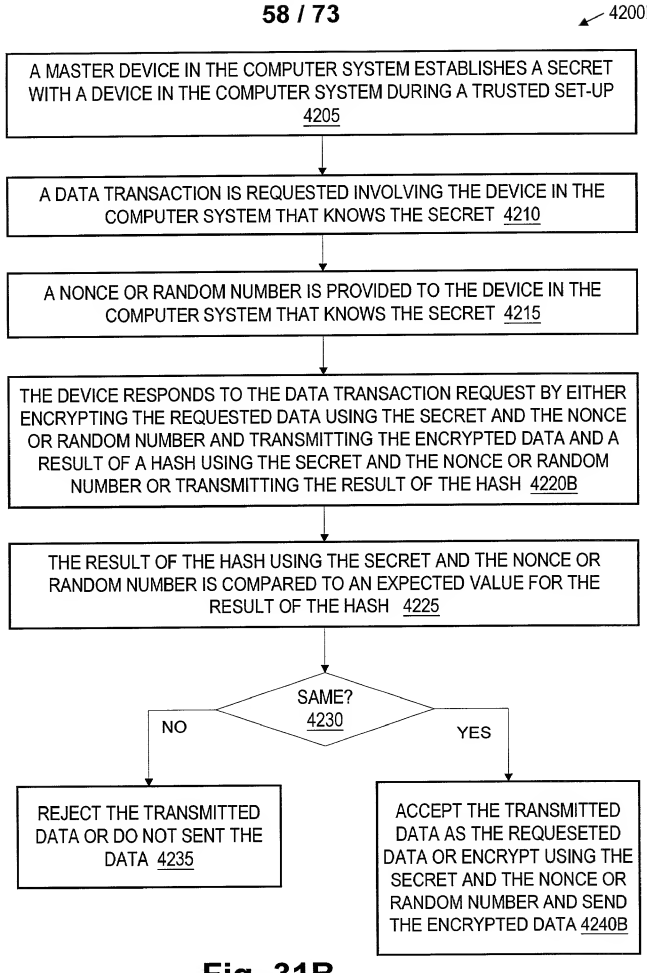
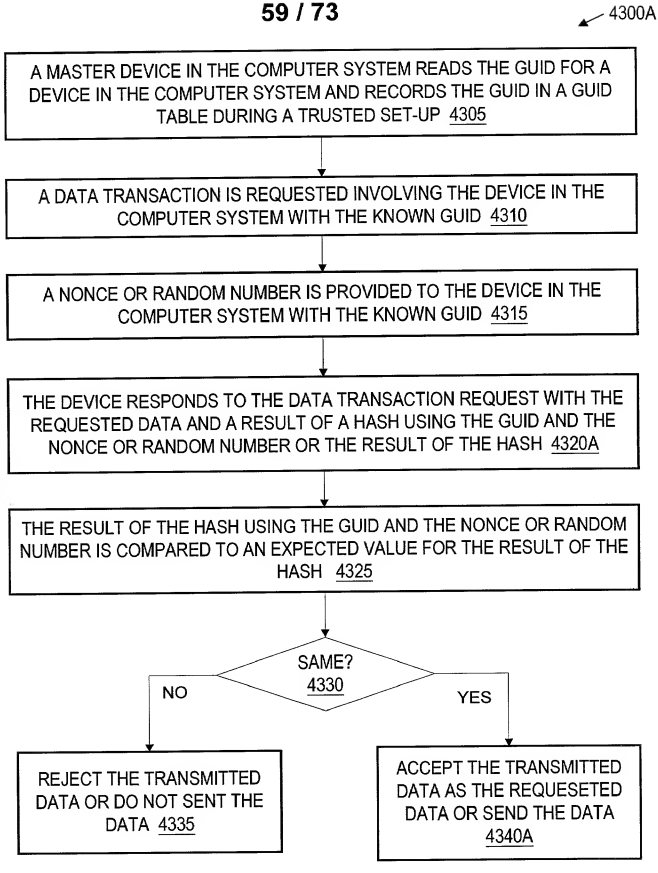


Fig. 31B

TT0850 06807860



TT0CE50"06804860

Fig. 32A

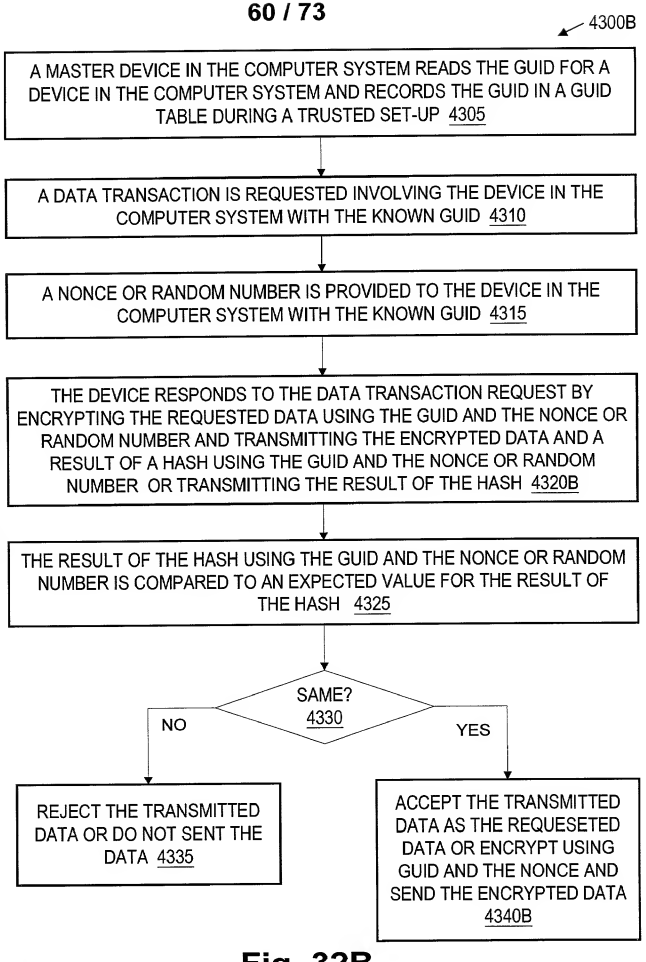


Fig. 32B

0980780 "05300L

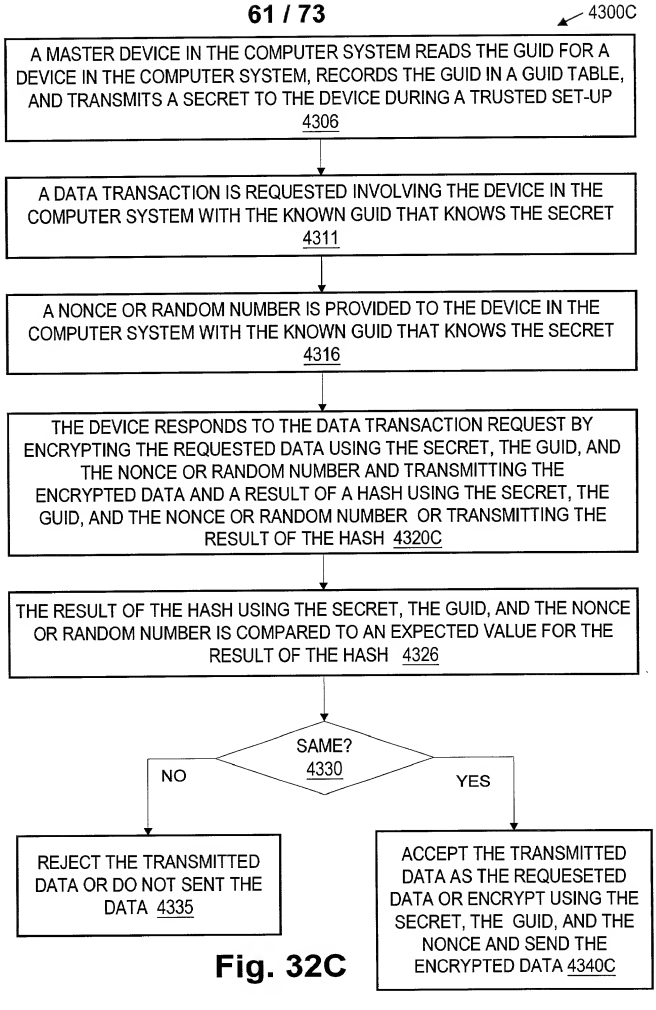


Fig. 32C

US 6,092,080 "05300"

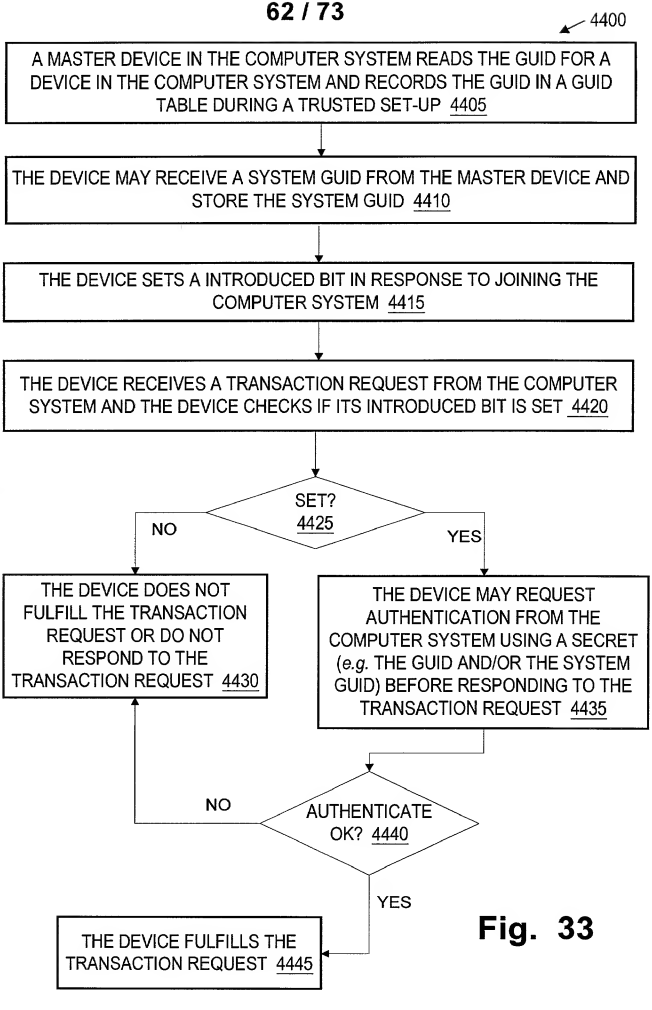


Fig. 33

0187.0890.053001

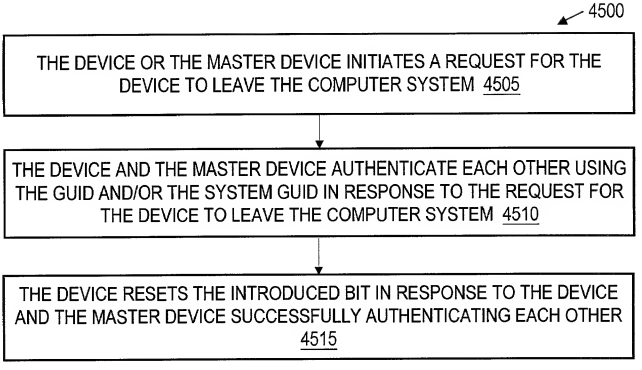


Fig. 34

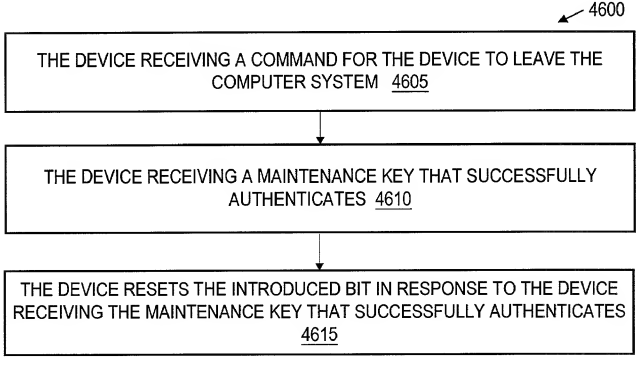


Fig. 35

0980708910.052001

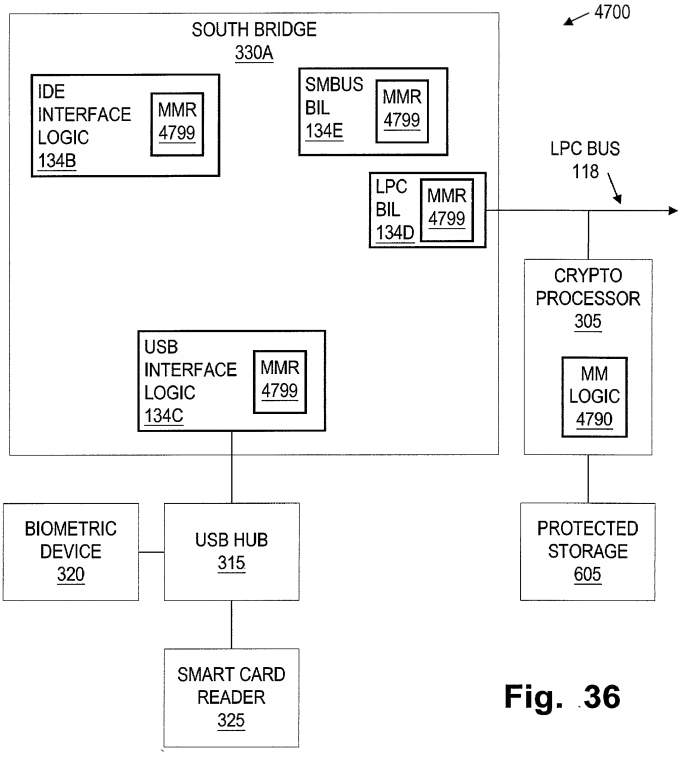
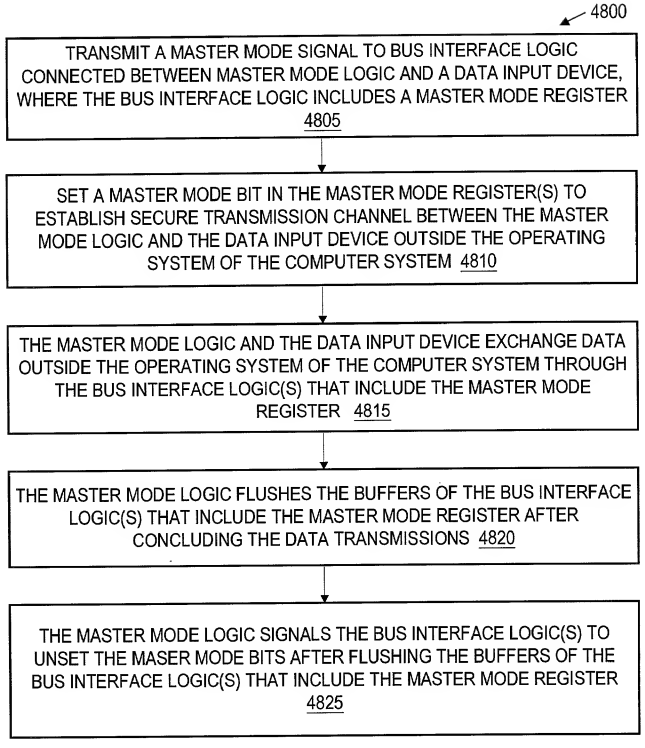


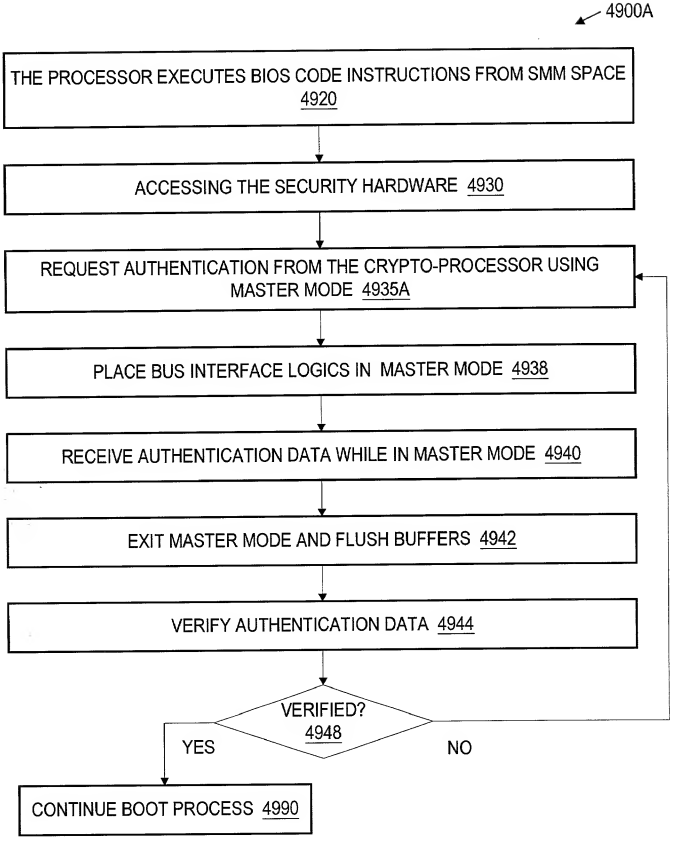
Fig. 36

TT0550 * 06/30/2004



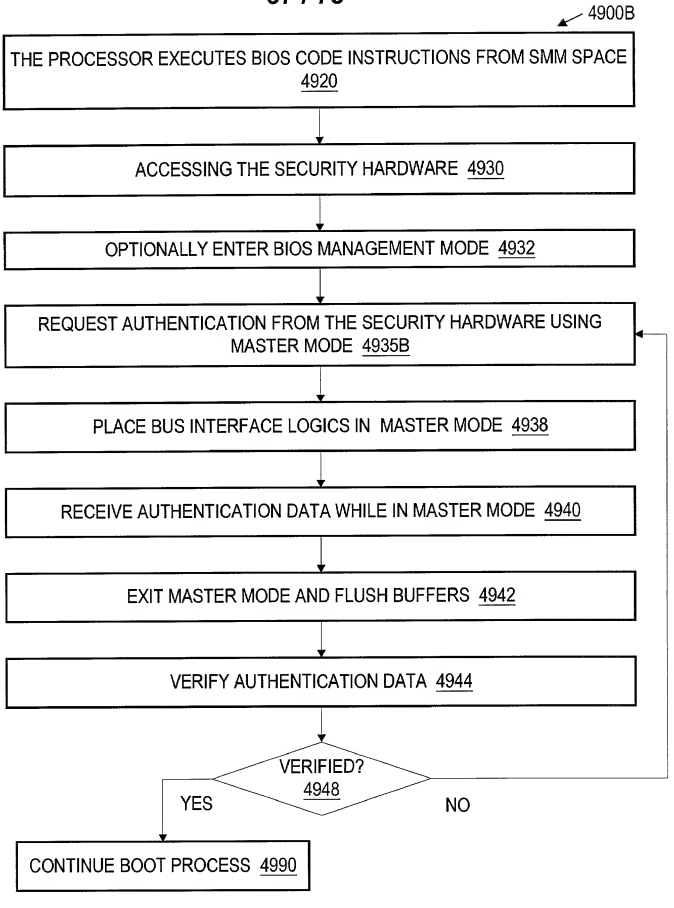
0990708900.052001

Fig. 37



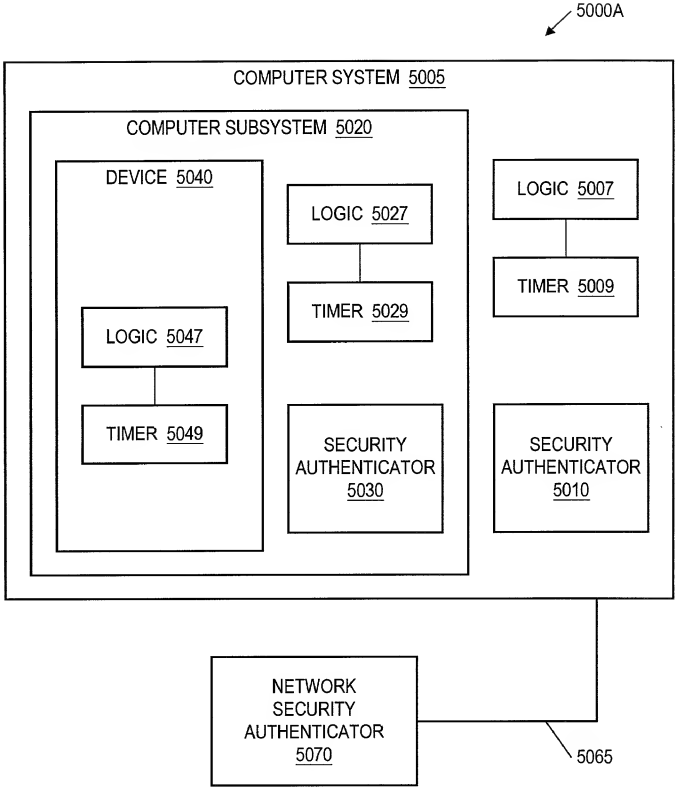
0987088D-0530D1

Fig. 38A



TT0ES0-06807860

Fig. 38B



09807890.053001

Fig. 39A

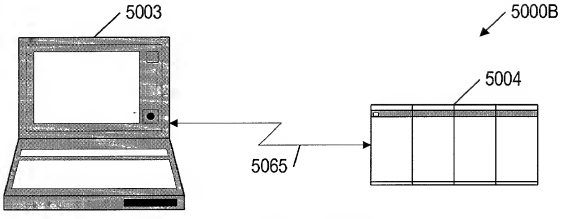


Fig. 39B

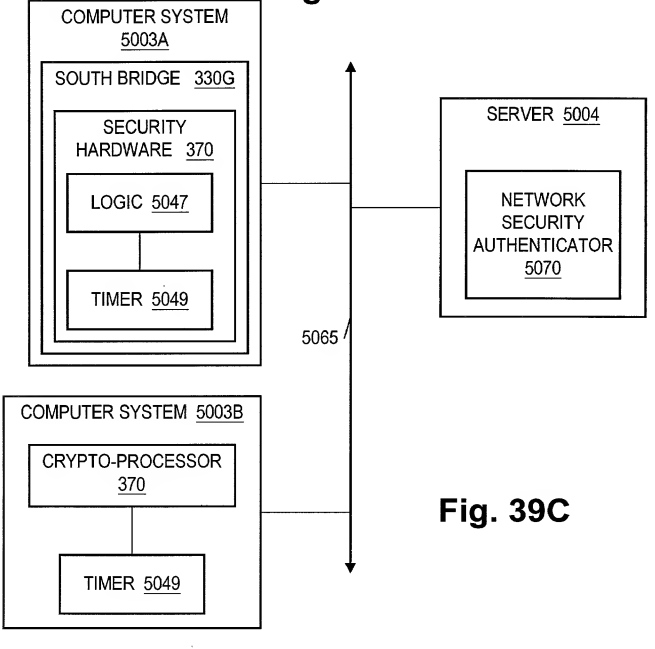


Fig. 39C

"05350.0680/4860

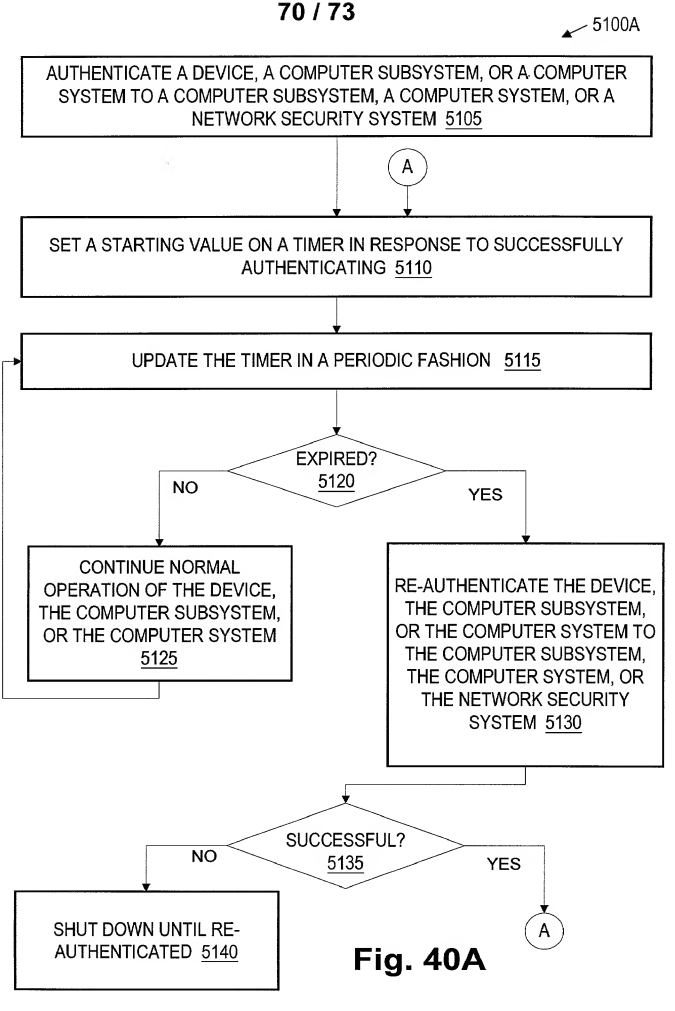


Fig. 40A

0987.0890.053001

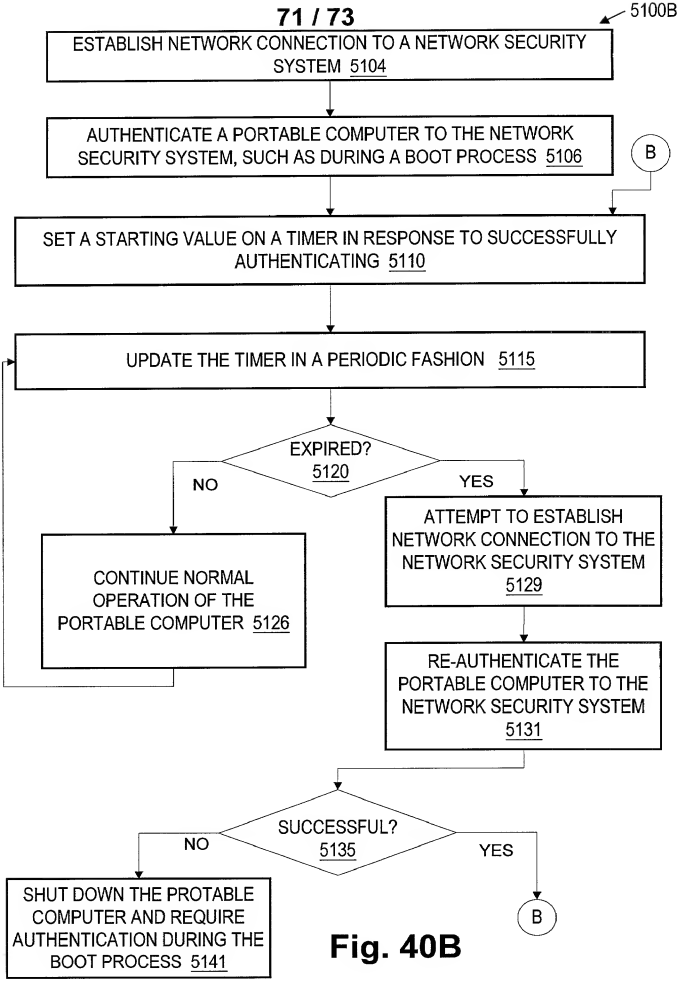


Fig. 40B

0980760 - 0530010

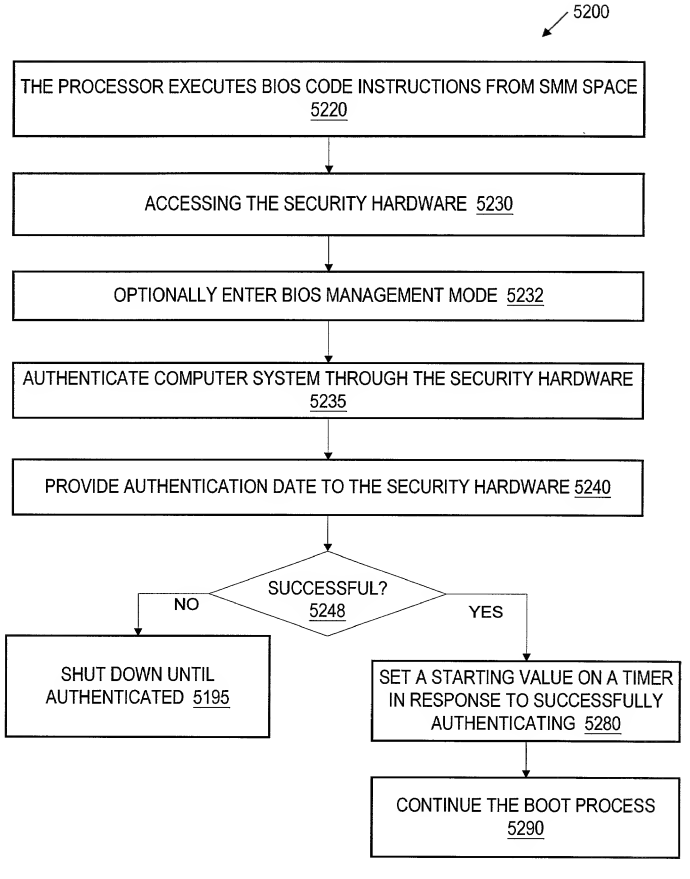

5200
THE PROCESSOR EXECUTES BIOS CODE INSTRUCTIONS FROM SMM SPACE 5220
ACCESSING THE SECURITY HARDWARE 5230
OPTIONALLY ENTER BIOS MANAGEMENT MODE 5232
AUTHENTICATE COMPUTER SYSTEM THROUGH THE SECURITY HARDWARE 5235
PROVIDE AUTHENTICATION DATE TO THE SECURITY HARDWARE 5240
SUCCESSFUL? 5248
NO
YES
SHUT DOWN UNTIL AUTHENTICATED 5195
SET A STARTING VALUE ON A TIMER IN RESPONSE TO SUCCESSFULLY AUTHENTICATING 5280
CONTINUE THE BOOT PROCESS 5290

Fig. 41

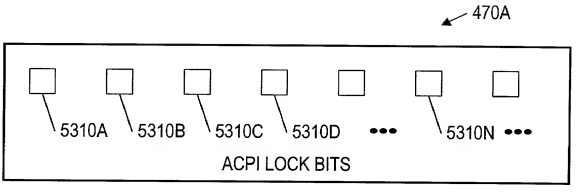


Fig. 42A

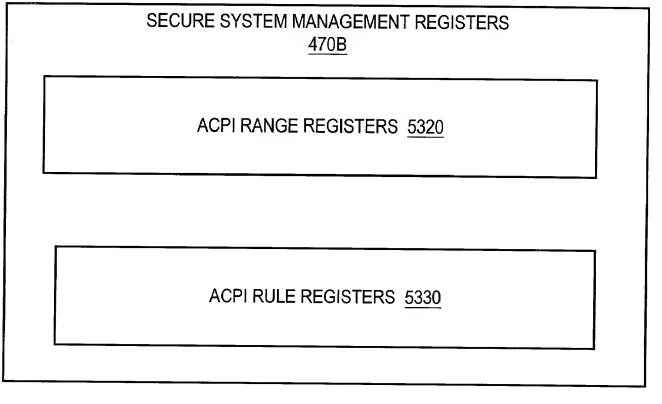


Fig. 42B

10030*05301